Semigroup Forum
https://doi.org/10.1007/s00233-020-10127-0

RESEARCH ARTICLE

On finitary properties for fiber products of free semigroups and free monoids

Ashley Clayton[1]

Received: 25 June 2019 / Accepted: 1 July 2020

Abstract
We consider necessary and sufficient conditions for finite generation and finite presentability for fiber products of free semigroups and free monoids. We give a necessary and sufficient condition on finite fiber quotients for a fiber product of two free monoids to be finitely generated, and show that all such fiber products are also finitely presented. By way of contrast, we show that fiber products of free semigroups over finite fiber quotients are never finitely generated. We then consider fiber products of free semigroups over infinite semigroups, and show that for such a fiber product to be finitely generated, the quotient must be infinite but finitely generated, idempotent-free, and $\mathcal{J}$-trivial. Finally, we construct automata accepting the indecomposable elements of the fiber product of two free monoids/semigroups over free monoid/semigroup fibers, and give a necessary and sufficient condition for such a product to be finitely generated.

Keywords Subdirect product · Fiber product · Semigroup · Free semigroup · Free monoid

Mathematics Subject Classification Primary: 20MO5 · Secondary: 08B26

1 Introduction

A *subdirect product* of two algebras A and B is a subalgebra of the direct product, for which the natural projections onto A and B are surjective. In particular, the direct product of two algebras is a subdirect product, for which finitary properties have been well studied for groups. Most results indicate that direct products of groups have a well behaved structure based on their constituent factors. That is,

Communicated by Victoria Gould.

✉ Ashley Clayton
ac323@st-andrews.ac.uk

1 School of Mathematics and Statistics, University of St Andrews, St Andrews, Scotland, UK

Published online: 14 August 2020

two groups G and H have the following properties (amongst others) if and only if $G \times H$ also does: finitely generated; finitely presented; residually finite; nilpotent; solvable; and having decidable word problem.

By way of contrast, subdirect products of groups have more complicated behaviour in general, which has been particularly well exhibited for subdirect products of free groups. There are examples (stemming from [1, Theorem 1]) which are not finitely generated [2, Example 3]; finitely generated without being finitely presented [6]; and finitely generated but with undecidable membership problem [10]. Describing their substructure complexity, any two non-abelian free groups G and H have uncountably many pairwise non-isomorphic subdirect products of G and H [2, Corollary B].

By a result due to Goursat [5], subdirect products of groups arise as fiber products and vice versa, and are hence constructible in some sense. By a comparatively more recent result due to Fleischer [3], this is also true more generally for varieties of algebras which are congruence permutable (that is, all congruences commute with each other under composition) and equivalently varieties whose languages contain Mal'cev terms, which include the varieties of groups, rings and Lie algebras. In varieties whose algebras do not contain Mal'cev terms however, fiber products are subdirect, but not conversely. It is natural to investigate the boundary between those subdirect products which are constructible via fiber products, and those which are not in such varieties.

Furthermore, the setting of the subdirect product structure in Universal Algebra owes itself to many natural questions relating to generation, presentation, and decidability for given varieties. The varieties of semigroups, monoids and lattices are not congruence permutable, and recent results indicate as for groups that subdirect products of the free objects in these varieties are already interesting. For example for the free monogenic semigroup viewed as $\mathbb{N}$, there are uncountably many pairwise non-isomorphic subdirect products of $\mathbb{N}^k$ for any $k \geq 2$ [4]. For questions of finite generation, Mayr and Ruškuc [9] have given some examples of the complications arising for free monoids: there exist fiber products of two free monogenic monoids over a finite fiber quotient which are not finitely generated [9, Example 7.1], and projection onto several factors is not sufficient for finite generation of subdirect products of more than two monoids [9, Example 7.3]. Following this, they ask the below question:

Question 1.1 ([9], Problem 7.2) Find necessary and sufficient conditions for a fiber product of finitely generated monoids over a finite monoid to be finitely generated. More specifically, is it decidable whether a fiber product of two finitely generated free monoids over a finite quotient is finitely generated?

Following this preceding work, in this paper we undertake an investigation into finite generation and presentation for fiber products of free semigroups and monoids. In Sect. 2, we introduce the necessary preliminary materials concerning subdirect products, fiber products, and formal language and automata theory. In Sect. 3, we consider fiber products of free semigroups and monoids over finite fiber quotients, answering Question 1.1 in this case. In particular, we give the following results:

- There are no finitely generated fiber products of two free semigroups over a finite fiber quotient (Proposition 3.1);
- It is decidable whether a fiber product of two finitely generated free monoids over a finite fiber quotient is finitely generated, and give necessary and sufficient conditions on the fiber quotient (Theorem 3.4);
- If a fiber product of two finitely generated free monoids over a finite fiber quotient is finitely generated, then it is also finitely presented (Theorem 3.5), and give a presentation in this case.

In Sect. 4, we consider necessary conditions for finite generation for fiber products of free semigroups and monoids over infinite fiber quotients. In particular, we show the following:

- Finitely generated fiber products of free semigroups have finitely generated, $\mathcal{J}$-trivial, idempotent-free fiber quotients (Lemma 4.1, Proposition 4.4, Proposition 4.5);
- A fiber product of free semigroups with fiber quotient $\mathbb{N}$ is finitely generated if and only if at least one of the epimorphisms maps the minimal generating set to a singleton image (Theorem 4.6);
- Fiber products of free semigroups over non-monogenic free commutative semigroup fiber quotients are not finitely generated (Example 4.7).

In Sect. 5, we consider decision problems on fiber products of free semigroups and monoids with free fiber quotients, showing the following:

- The generalised word problem for a fiber product of semigroups in the direct product is decidable if and only if the word problem of the fiber quotient is decidable;
- Given a fiber product of two free semigroups (monoids) over a free semigroup (monoid) fiber quotient, one can ask whether or not it is finitely generated. This finite generation problem is decidable, for which we construct suitable finite state automata (Theorem 5.6, Corollary 5.12).

In Sect. 6, we make some remarks on the number of finitely generated subdirect products of two free semigroups A^+ and B^+, which are generated by some subset of $A \times B$. In particular, we count the number of such subdirect products (Proposition 6.1) as well as the number of fiber products (Proposition 6.2), and make some remarks on their sparsity in $A^+ \times B^+$.

Finally, we conclude in Sect. 7 with some arising open questions.

2 Preliminaries

Throughout, a *subdirect product of semigroups (resp. monoids)* S and T is a subsemigroup (resp. submonoid) U of $S \times T$ such that the projection maps

$$\pi_S : U \to S, \; \pi_T : U \to T$$

are surjections. In this case, we write $U \leq_{\mathrm{sd}} S \times T$. This definition naturally extends to a *subdirect product of a family of semigroups (resp. monoids)* $\{S_i\}_{i \in I}$, being a subsemigroup (resp. submonoid) U of the direct product $\prod_{i \in I} S_i$ for which each of the projection maps $\pi_i : U \to S_i$ are surjections. For this paper however, we only consider finite families.

If $\varphi : S \to F$, $\psi : T \to F$ are two epimorphisms onto a common semigroup (resp. monoid) F, then the *fiber product of S and T with respect to* φ, ψ is the subdirect product of $S \times T$ given by the set

$$\{(s, t) \in S \times T : \varphi(s) = \psi(t)\},$$

with multiplication inherited from $S \times T$. We will write $\Pi(\varphi, \psi)$ to denote the fiber product. The semigroup F is called the *fiber quotient* of the fiber product. Similarly to subdirect products, fiber products can be defined on families of semigroups and monoids as well. Fiber products are indeed subdirect products of S and T, but not all subdirect products can be obtained in this way. The following result classifies when the two notions coincide:

Lemma 2.1 (cf. Fleischer's Lemma [3], Lemma 10.1]) *Let S, T be semigroups, let $U \leq_{\mathrm{sd}} S \times T$. Then U is a fiber product if and only if the kernel congruences of the projection maps π_S and π_T commute under composition. That is, if*

$$\ker \pi_S \circ \ker \pi_T = \ker \pi_T \circ \ker \pi_S.$$

An *alphabet* is a set A consisting of formal symbols, where the elements of A are referred to as *letters*. The *free semigroup* A^+ is the set of all finite non-empty strings of letters over A, with the operation of concatenation of strings. Allowing for the empty string ε (being the string consisting of no letters), the *free monoid* A^* is the set of all finite strings over A, again with the operation of concatenation. A *word* over A is an element of A^*. The empty string ε is called the *empty word*. For a word $w \in A^+$, we will write w_i for the i-th letter of w. A *prefix* of a word $w \in A^*$ is an element $u \in A^*$ such that there exists $v \in A^*$ with $w = uv$. A *proper prefix* u of $w \in A^*$ is a prefix which is not equal to w. If u is a prefix of w, we will write $u \leq_p w$, and $u <_p w$ if u is a proper prefix, in particular. Similarly, a *suffix* of a word $w \in A^*$ is an element $v \in A^*$ such that there exists $u \in A^*$ with $w = uv$, and a *proper suffix* of $w \in A^*$ is a suffix v not equal to w. If v is a suffix of w, we will write $v \leq_s w$, and $v <_s w$ if v is a proper suffix, in particular. For a prefix u (resp. suffix v) of w, we write $u^{-1}w$ (resp. wv^{-1}) to mean the unique word u' (resp. v') such that $uu' = w$ (resp. $v'v = w$), or equivalently the word w with prefix u (resp. suffix v) removed.

For a semigroup S, an *idempotent* is an element $e \in S$ such that $e^2 = e$. The set of all idempotents of a semigroup is denoted $E(S)$. A semigroup S will be called *idempotent-free* if $E(S) = \emptyset$. An element s of a semigroup S is called *semigroup indecomposable* if there are no $s_1, s_2 \in S$ such that $s = s_1 s_2$ (and is otherwise called *semigroup decomposable*). Similarly, an element m of a monoid M is called *monoid indecomposable* if there are no $m_1, m_2 \in M \setminus \{1_M\}$ such that $m = m_1 m_2$ (and is otherwise called *monoid decomposable*). When the context is clear, we will refer to semigroup and monoid decomposability simply as decomposability.

For a semigroup S, let 1 be a symbol not in S, and define $S^1 := S$ if S has an identity, and $S \cup \{1\}$ otherwise, where 1 acts as an identity on S. *Green's relations* $\mathcal{R}, \mathcal{L}, \mathcal{H}, \mathcal{J}$ are the equivalence relations on S that can be given by the following:

$$\begin{aligned}
(s,t) \in \mathcal{R} &\Leftrightarrow (\exists x, y \in S^1)(s = tx)(t = sy);\\
(s,t) \in \mathcal{L} &\Leftrightarrow (\exists x, y \in S^1)(s = xt)(t = ys);\\
(s,t) \in \mathcal{H} &\Leftrightarrow (s,t) \in \mathcal{R} \cap \mathcal{L};\\
(s,t) \in \mathcal{J} &\Leftrightarrow (\exists x, x', y, y' \in S^1)(s = xty)(t = x'sy').
\end{aligned}$$

For $\mathcal{K} \in \{\mathcal{R}, \mathcal{L}, \mathcal{H}, \mathcal{J}\}$, we say that a semigroup S is $\mathcal{K}$*-trivial* if $\mathcal{K} = \{(s,s) : s \in S\}$. Note that as $\mathcal{H} \subseteq \mathcal{R} \subseteq \mathcal{J}$ and $\mathcal{H} \subseteq \mathcal{L} \subseteq \mathcal{J}$, in particular if a semigroup is $\mathcal{J}$-trivial, it is also $\mathcal{R}$-trivial, $\mathcal{L}$-trivial and $\mathcal{H}$-trivial.

A semigroup S is said to be *finitely generated* if there exists a finite subset X of S such that $S = \langle X \rangle$, i.e the elements of S are expressible as finite products of elements in X. Given a semigroup S and $X \subseteq S$ a finite generating set, the *word problem of* S with respect to X is given by

$$\mathrm{WP}(S,X) = \{(u,v) \in X^+ \times X^+ : u =_S v\},$$

where $u =_S v$ means u and v represent the same element in S. Specifically, $u =_S v$ means $\pi(s) = \pi(v)$, where $\pi : X^+ \to S$ is the unique morphism from X^+ to S such that $\pi(x) = x$, for all $x \in X$. The word problem of S is said to be *decidable* with respect to X if there exists an algorithm taking S, a finite generating set $X \subseteq S$ and any $(u,v) \in X^+ \times X^+$ as inputs which determines whether or not $(u,v) \in \mathrm{WP}(S,X)$.

Given a finitely generated semigroup S, a finitely generated subsemigroup T of S and a generating set X for S, the *generalized word problem of* T *in* S is the set of words over X which represent an element in T. More specifically, it is the set $X^+ \cap \pi^{-1}(T)$, where $\pi : X^+ \to S$ is the unique morphism from X^+ to S such that $\pi(x) = x$, for all $x \in X$. The generalized word problem is said to be decidable if there is an algorithm taking S, X and a finite subset Y of X^* generating T, which decides whether or not a word w over X represents an element in $\langle Y \rangle$.

We use the notation $\mathrm{Gp}\langle X : R \rangle$, $\mathrm{Mon}\langle X : R \rangle$ to differentiate between group presentations and monoid presentations, respectively, with generating set X and relations R (more detail on presentations can be found in [7]).

Finally, by convention $\mathbb{N}$ will denote the set of natural numbers $\{1, 2, \dots\}$ *not* including 0. The set $\{0, 1, 2, \dots\}$ will be denoted by $\mathbb{N}^0$.

3 Fiber products of free semigroups/monoids over finite fiber quotients

This section is devoted to classifying the finite fiber quotients and associated epimorphisms φ, ψ with free semigroup/monoid domains for which $\Pi(\varphi, \psi)$ is finitely generated.

We begin by showing in the free semigroup case, there are no such fiber quotients.

Proposition 3.1 *Let $\varphi : A^+ \to S$, $\psi : B^+ \to S$ be epimorphisms where S is a finite semigroup. Then the fiber product $\Pi(\varphi, \psi)$ of A^+ with B^+ over S with respect to φ, ψ is not finitely generated.*

Proof Let $(u, v) \in \Pi(\varphi, \psi)$. Let $s = \varphi(u) = \psi(v)$. As S is finite, there exists some $k \in \mathbb{N}$ such that s^k is idempotent. Hence $(u^k, v^{nk}) \in \Pi(\varphi, \psi)$ for all $n \in \mathbb{N}$.

Suppose for a contradiction that $X = \{(u_i, v_i) : 1 \leq i \leq p\} \subseteq A^+ \times B^+$ were a finite generating set for $\Pi(\varphi, \psi)$. Then as u^k can be decomposed into at most $k|u|$ factors in A^+, it follows that each pair (u^k, v^{nk}) can be decomposed into at most $k|u|$ factors in $\langle X \rangle$. This is a contradiction, as this implies that $|v^{nk}| \leq k|u| \max_{1 \leq i \leq p} |v_i|$ for all $n \in \mathbb{N}$. Hence $\Pi(\varphi, \psi)$ is not finitely generated. ☐

We note that the above result can also be obtained as a corollary of Proposition 4.4 seen later, as any finite image S has idempotents. For the remainder of this section, we work towards giving necessary and sufficient conditions for fiber products of two finitely generated free monoids over finite fiber quotients to be finitely generated. Our next lemma shows that such quotients are necessarily restricted to the class of finite groups.

Lemma 3.2 *Let $\varphi : A^* \to M$, $\psi : B^* \to M$ be epimorphisms onto a finite monoid M. If M is not a group, then $\Pi(\varphi, \psi)$ is not finitely generated.*

Proof $\psi(B)$ is a generating set for M by surjectivity. As M is finite monoid which is not a group, then there exists some $m \in \psi(B)$ and $k \in \mathbb{N}$ such that m^k is idempotent, but $m^k \neq 1_M$.

As φ and ψ are surjections, then there exists a word $u \in A^*$ and a letter $b \in B$ such that $\varphi(u) = m = \psi(b)$. Hence $\{(u^k, b^{nk}) : n \in \mathbb{N}\} \subseteq \Pi(\varphi, \psi)$.

Suppose for a contradiction that $X = \{(u_i, v_i) : 1 \leq i \leq p\} \subseteq A^* \times B^*$ were a finite generating set for $\Pi(\varphi, \psi)$. As $\psi(b^j) \neq 1_M$ for all $j \in \mathbb{N}$ then it follows that $(\varepsilon, b^j) \notin \Pi(\varphi, \psi)$ for all $j \in \mathbb{N}$, hence we must have $(u^k, b^{nk}) \in \langle X' \rangle$ for all $n \in \mathbb{N}$, where $X' = \{(u_i, v_i) \in X : u_i \neq \varepsilon\}$. Then as u^k can be decomposed into at most $k|u|$ non-empty factors in X^*, it follows that each pair (u^k, b^{nk}) can be decomposed into at most $k|u|$ factors in $\langle X' \rangle$. This is a contradiction, as this implies that $|b^{nk}| \leq k|u| \max_{1 \leq i \leq p} |v_i|$ for all $n \in \mathbb{N}$. Hence $\Pi(\varphi, \psi)$ is not finitely generated. ☐

Our next lemma refines the previous result, to show that the fiber quotients of interest must be cyclic groups.

Lemma 3.3 *Let $\varphi : A^* \to G, \psi : B^* \to G$ be epimorphisms where G is a finite non-cyclic group. Then $\Pi(\varphi, \psi)$ is not finitely generated.*

Proof $\psi(B)$ is a finite generating set for the group G by surjectivity. As G is not cyclic, then there exist elements $g, h \in \psi(B)$ such that

$$gh^p \neq 1_G \quad \text{for all } p \in \mathbb{N}, \tag{1}$$

for otherwise there exists $x \in \psi(B)$ such that, for any $g \in \psi(B)$, there is some $i \in \mathbb{N}$ with $g = (x^{-1})^i$, contradicting that G is non-cyclic. By surjectivity, there exist distinct letters $a, b \in B$ such that $\psi(a) = g$ and $\psi(b) = h$. In particular, $\psi(ab^p) \neq 1_G$ for any $p \in \mathbb{N}$ by (1).

As G is a finite group, let j, k denote the orders of the elements g, h respectively. Then it follows that $\psi(ab^{nk}a^{j-1}) = 1_G$ for all $n \in \mathbb{N}$. Hence

$$\{(\varepsilon, ab^{nk}a^{j-1}) : n \in \mathbb{N}\} \subseteq \Pi(\varphi, \psi).$$

We claim that $(\varepsilon, ab^{nk}a^{j-1})$ is indecomposable in $\Pi(\varphi, \psi)$ for any $n \in \mathbb{N}$. Suppose for a contradiction that we have a non-trivial decomposition

$$(\varepsilon, ab^{nk}a^{j-1}) = (u_1, v_1)(u_2, v_2)$$

for some $(u_1, v_1), (u_2, v_2) \in \Pi(\varphi, \psi) \setminus \{(\varepsilon, \varepsilon)\}$. Clearly, it must be the case that $u_1 = u_2 = \varepsilon$. As the composition is non-trivial, then v_1 is non-empty, and a must be a prefix of v_1. As $\psi(a) \neq 1_G$, but $\psi(v_1) = \varphi(u_1) = 1_G$, then $v_1 \neq a$ in particular and hence ab is a prefix of v_1. Similarly as $\psi(ab^p) \neq 1_G$ for any $p \in \mathbb{N}$, it follows that $ab^{nk}a$ is a prefix of v_1. Finally, as $\psi(ab^{nk}a^p) \neq 1_G$ for any $1 \leq p < j-1$, it must be that $v_1 = ab^{nk}a^{j-1}$. But it now follows that $(u_2, v_2) = (\varepsilon, \varepsilon)$, a contradiction. Hence the claim is proved, and as any generating set for $\Pi(\varphi, \psi)$ must contain the indecomposable elements of $\Pi(\varphi, \psi)$, then $\Pi(\varphi, \psi)$ is not finitely generated. □

Finally, we give all conditions on finite fiber quotients and epimorphisms for which the associated fiber product of two free monoids is finitely generated.

Theorem 3.4 *Let $\varphi : A^* \to F$, $\psi : B^* \to F$ be epimorphisms where F is a finite monoid. Then the fiber product of A^* with B^* over F with respect to φ, ψ is finitely generated if and only if A and B are finite, $|\varphi(A)| = |\psi(B)| = 1$, F is a cyclic group.*

Proof ($\Rightarrow$) If A is infinite, then A^* is not finitely generated and hence neither is $\Pi(\varphi, \psi)$, for otherwise projection from such a finite generating set onto the first coordinate would give a finite generating set for A^*. The same reasoning applies for if B is infinite.

If F is not a cyclic group, then $\Pi(\varphi, \psi)$ is not finitely generated by Lemmas 3.2 and 3.3. Otherwise, let F be the finite cyclic group generated by element $x \in F$ of order k (that is, $F \cong \mathrm{Gp}\langle x : x^k = 1\rangle$), and suppose $\varphi : A^* \to F$ is such that $|\varphi(A)| > 1$. Then $\varphi(a) \neq \varphi(a')$ for some $a, a' \in A$, and we can choose $a_1 \in \{a, a'\}$

such that $\varphi(a_1) \neq 1$. We can also choose $a_2 \in \{a, a'\}$ such that $\varphi(a_1 a_2) \neq 1$, for otherwise $\varphi(a_1 a) = \varphi(a_1 a')$ implies $\varphi(a) = \varphi(a')$.

Repeating this process, we can construct for each $n \in \mathbb{N}$ a word $u_n = a_1 a_2 \dots a_n \in A^+$ such that $\varphi(a_1 a_2 \dots a_m) \neq 1$ for $1 \leq m \leq n$. Letting $g = \varphi(u_n)$, there exists some $v_n \in A^+$ of minimal length such that $g^{-1} = \varphi(v_n)$. Letting $w_n = u_n v_n$, then it follows that $\varphi(w_n) = 1$, but $\varphi(w) \neq 1$ for any proper prefix $w <_p w_n$. Consider the sequence $\{i_j\}_{j \in \mathbb{N}} \subseteq \mathbb{N}$ given by $i_1 = 1$, and $i_{j+1} = |w_{i_j}| + 1$ for $j \geq 1$. Then the sequence of words $\{w_{i_j}\}_{j \in \mathbb{N}} \subseteq A^+$ is such that, for each $j \in \mathbb{N}$, $|w_{i_j}| < |w_{i_{j+1}}|$, and $\varphi(w_{i_j}) = 1$, but $\varphi(w) \neq 1$ for any proper prefix $w <_p w_{i_j}$. It then follows that

$$\{(w_{i_j}, \varepsilon) : j \in \mathbb{N}\} \subseteq \Pi(\varphi, \psi)$$

is an infinite set of distinct indecomposable pairs of $\Pi(\varphi, \psi)$. As any generating set for $\Pi(\varphi, \psi)$ must contain all the indecomposable elements of $\Pi(\varphi, \psi)$, it follows that $\Pi(\varphi, \psi)$ is not finitely generated.

If $|\psi(B)| > 1$ is such that $\psi(b) \neq \psi(b')$ for some $b, b' \in B$, then the same argument also shows that $\Pi(\varphi, \psi)$ is not finitely generated.

($\Leftarrow$) Suppose that A and B are finite, F is a cyclic group, and $|\varphi(A)| = |\psi(B)| = 1$. Then F has a group presentation $F = \mathrm{Gp}\langle x : x^n = 1 \rangle$ for some $n \in \mathbb{N}$, and $\varphi(A) = \{x^p\}$, $\psi(B) = \{x^q\}$ for some $1 \leq p, q \leq n$ with $\gcd(p, n) = \gcd(q, n) = 1$. If $(u, v) \in \Pi(\varphi, \psi)$, then

$$\begin{aligned} & \varphi(u) = \psi(v) \\ \Leftrightarrow & (x^p)^{|u|} = (x^q)^{|v|} \\ \Leftrightarrow & x^{p|u|} = x^{q|v|} \\ \Leftrightarrow & p|u| \,(\mathrm{mod}\, n) = q|v| \,(\mathrm{mod}\, n). \end{aligned}$$

Hence

$$\Pi(\varphi, \psi) = \{(u, v) \in A^* \times B^* : p|u| \equiv q|v| \,(\mathrm{mod}\, n)\}.$$

We claim that $\Pi(\varphi, \psi)$ is finitely generated by

$$\begin{aligned} X = & \{(u, v) \in A^* \times B^* : p|u| \equiv q|v| \,(\mathrm{mod}\, n), 0 \leq |u|, |v| \leq n\} \\ & \setminus \{(u, v) \in A^* \times B^* : |u| = |v| = n\}. \end{aligned}$$

Let $(u, v) \in \Pi(\varphi, \psi)$. Let p' be such that $pp' \equiv 1 \,(\mathrm{mod}\, n)$, and let q' be such that $qq' \equiv 1 \,(\mathrm{mod}\, n)$. Then as $|u| = k_1 n + r_1$ for some $0 \leq r_1 < n$ with $r_1 \equiv p'q|v| \,(\mathrm{mod}\, n)$, $k_1 \in \mathbb{N}^0$, and $|v| = k_2 n + r_2$ for some $0 \leq r_2 < n$ with $r_2 \equiv q'p|u| \,(\mathrm{mod}\, n)$, $k_2 \in \mathbb{N}^0$, it follows that

$$u = u' x_1 x_2 \dots x_{k_1}$$

for some $u', x_i \in A^*$ with $|u'| = r_1$, $|x_i| = n$ for $1 \leq i \leq k_1$, and similarly

$$v = v' y_1 y_2 \dots y_{k_2}$$

for some $v', y_i \in B^*$ with $|v'| = r_2, |y_i| = n$ for $1 \leq i \leq k_2$. Then we have:

- $(u', v') \in X$, as $0 \leq |u'|, |v'| < n$, and
$$p|u'| = pr_1 \equiv pp'q|v| \equiv q|v| \equiv qr_2 \equiv q|v'| \pmod n;$$
- $(x_i, \varepsilon) \in X$ for all $1 \leq i \leq k_1$, as $p|x_i| \equiv 0 \equiv q|\varepsilon| \pmod n$;
- $(\varepsilon, y_i) \in X$ for all $1 \leq i \leq k_2$, as $q|y_i| \equiv 0 \equiv p|\varepsilon| \pmod n$.

Hence

$$(u, v) = (u', v')(x_1, \varepsilon) \dots (x_{k_1}, \varepsilon)(\varepsilon, y_1) \dots (\varepsilon, y_{k_2}) \in \langle X \rangle,$$

proving the claim. □

Theorem 3.5 *Let $\varphi : A^* \to F$, $\psi : B^* \to F$ be epimorphisms where F is a finite monoid. If the fiber product of A^* with B^* over F with respect to φ, ψ is finitely generated, then it is is also finitely presented.*

We introduce the next two lemmas in order to prove Theorem 3.5:

Lemma 3.6 *Let $\varphi : A^* \to F$, $\psi : B^* \to F$ be epimorphisms where $F = \mathrm{Gp}\langle x : x^n = 1 \rangle$, satisfying $\varphi(A) = \{x^p\}, \psi(B) = \{x^q\}$ for some $1 \leq p, q \leq n$ with $\gcd(p, n) = \gcd(q, n) = 1$. Let*

$$\bar{\Gamma} := \{\gamma(u, v) : u \in A^*, v \in B^*,\ p|u| \equiv q|v| \pmod n,\ 0 \leq |u|, |v| \leq n\}$$

and

$$\Gamma := \bar{\Gamma} \setminus \{\gamma(u, v) : u \in A^*, v \in B^*, |u| = |v| = n \text{ or } |u| = |v| = 0\}$$

be sets of formal symbols. Then the relations (for $u, u_1, u_2, u_3 \in A^*$, $v, v_1, v_2, v_3 \in B^*$) given by

$$(\gamma(\varepsilon, v)\gamma(u, \varepsilon),\ \gamma(u, \varepsilon)\gamma(\varepsilon, v)) \qquad (|u| = |v| = n); \tag{R1}$$

$$(\gamma(\varepsilon, v)\gamma(u, v_1),\ \gamma(u, v_2)\gamma(\varepsilon, v_3)) \ \begin{array}{r}(0 < |u|, |v_1| < n, |v| = |v_3| = n,\\ p|u| \equiv q|v_1| \pmod n, vv_1 = v_2v_3);\end{array} \tag{R2}$$

$$(\gamma(u, \varepsilon)\gamma(u_1, v),\ \gamma(u_2, v)\gamma(u_3, \varepsilon)) \ \begin{array}{r}(0 < |v|, |u_1| < n, |u| = |u_3| = n,\\ p|u_1| \equiv q|v| \pmod n, uu_1 = u_2u_3)\end{array} \tag{R3}$$

over Γ hold in $\Pi(\varphi, \psi)$.

Proof We note first that for $\gamma(u, v) \in \Gamma$, it follows that $|u| = n$ if and only if $|v| = 0$, and similarly $|u| = 0$ if and only if $|v| = n$. Let $\bar{\pi} : \Gamma \to \Pi(\varphi, \psi)$ be given by

$\bar{\pi}(\gamma(u,v)) = (u,v)$, and let $\pi : \Gamma^* \to \Pi(\varphi,\psi)$ be the unique homomorphism extending $\bar{\pi}$. Then in the case of (R1), we have

$$\pi(\gamma(\varepsilon,v)\gamma(u,\varepsilon)) = (\varepsilon,v)(u,\varepsilon) = (u,v) = (u,\varepsilon)(\varepsilon,v) = \pi(\gamma(u,\varepsilon)\gamma(\varepsilon,v)),$$

and so (R1) holds in $\Pi(\varphi,\psi)$. In the case of (R2), we have

$$\begin{aligned}\pi(\gamma(\varepsilon,v)\gamma(u,v_1)) &= (\varepsilon,v)(u,v_1)\\ &= (u,vv_1)\\ &= (u,v_2v_3)\\ &= (u,v_2)(\varepsilon,v_3)\\ &= \pi(\gamma(u,v_2)\gamma(\varepsilon,v_3)),\end{aligned}$$

and hence (R2) holds in $\Pi(\varphi,\psi)$. In the case of (R3), we have

$$\begin{aligned}\pi(\gamma(u,\varepsilon)\gamma(u_1,v)) &= (u,\varepsilon)(u_1,v)\\ &= (uu_1,v)\\ &= (u_2u_3,v)\\ &= (u_2,v)(u_3,\varepsilon)\\ &= \pi(\gamma(u_2,v)\gamma(u_3,\varepsilon)),\end{aligned}$$

and hence (R3) holds in $\Pi(\varphi,\psi)$. □

Lemma 3.7 *Let φ, ψ and Γ be as in Lemma 3.6. Let $\gamma(u_1,v_1),\gamma(u_2,v_2) \in \Gamma$ with $0 < |u_1|,|u_2| < n$, and define $u_3,u_4 \in A^*$, $v_3,v_4 \in B^*$ as follows:*

$$\begin{aligned}u_1u_2 &= u_3u_4, \qquad |u_4| = n \quad \text{if } |u_1u_2| > n,\\ v_1v_2 &= v_3v_4, \qquad |v_4| = n \quad \text{if } |v_1v_2| > n.\end{aligned}$$

Then the relation

$$(\gamma(u_1,v_1)\gamma(u_2,v_2),\ w) \tag{R4}$$

where

$$w = \begin{cases}\gamma(u_1u_2,v_1v_2) & \text{if } |u_1u_2|,|v_1v_2| < n,\\ \gamma(u_3,v_1v_2)\gamma(u_4,\varepsilon) & \text{if } |u_1u_2| > n, |v_1v_2| < n,\\ \gamma(u_1u_2,v_3)\gamma(\varepsilon,v_4) & \text{if } |u_1u_2| < n, |v_1v_2| > n,\\ \gamma(u_3,v_3)\gamma(u_4,\varepsilon)\gamma(\varepsilon,v_4) & \text{if } |u_1u_2|,|v_1v_2| > n,\\ \gamma(u_1u_2,\varepsilon)\gamma(\varepsilon,v_1v_2) & \text{if } |u_1u_2| = |v_1v_2| = n\end{cases}$$

over Γ holds in $\Pi(\varphi,\psi)$.

Proof Let $\bar{\pi} : \Gamma \to \Pi(\varphi,\psi)$ be given by $\bar{\pi}(\gamma(u,v)) = (u,v)$, and let $\pi : \Gamma^* \to \Pi(\varphi,\psi)$ be the unique homomorphism extending $\bar{\pi}$. For $\gamma(u_1,v_1),\gamma(u_2,v_2) \in \Gamma$ with $0 < |u_1|,|u_2| < n$, if $|u_1u_2|,|v_1v_2| < n$, then

$$\pi(\gamma(u_1,v_1)\gamma(u_2,v_2)) = (u_1,v_1)(u_2,v_2) = (u_1u_2,v_1v_2) = \pi(\gamma(u_1u_2,v_1v_2)).$$

If $|u_1u_2| > n, |v_1v_2| < n$, then

$$\begin{aligned}\pi(\gamma(u_1,v_1)\gamma(u_2,v_2)) &= (u_1,v_1)(u_2,v_2)\\ &= (u_1u_2,v_1v_2)\\ &= (u_3u_4,v_1v_2)\\ &= (u_3,v_1v_2)(u_4,\varepsilon)\\ &= \pi(\gamma(u_3,v_1v_2)\gamma(u_4,\varepsilon)).\end{aligned}$$

If $|u_1u_2| < n, |v_1v_2| > n$, then

$$\begin{aligned}\pi(\gamma(u_1,v_1)\gamma(u_2,v_2)) &= (u_1,v_1)(u_2,v_2)\\ &= (u_1u_2,v_1v_2)\\ &= (u_1u_2,v_3v_4)\\ &= (u_1u_2,v_3)(\varepsilon,v_4)\\ &= \pi(\gamma(u_1u_2,v_3)\gamma(\varepsilon,v_4)).\end{aligned}$$

If $|u_1u_2|, |v_1v_2| > n$, then

$$\begin{aligned}\pi(\gamma(u_1,v_1)\gamma(u_2,v_2)) &= (u_1,v_1)(u_2,v_2)\\ &= (u_1u_2,v_1v_2)\\ &= (u_3u_4,v_3v_4)\\ &= (u_3,v_3)(u_4,\varepsilon)(\varepsilon,v_4)\\ &= \pi(\gamma(u_3,v_3)\gamma(u_4,\varepsilon)\gamma(\varepsilon,v_4)).\end{aligned}$$

Finally if $|u_1u_2| = |v_1v_2| = n$, then

$$\begin{aligned}\pi(\gamma(u_1,v_1)\gamma(u_2,v_2)) &= (u_1,v_1)(u_2,v_2)\\ &= (u_1u_2,v_1v_2)\\ &= (u_1u_2,\varepsilon)(\varepsilon,v_1v_2)\\ &= \pi(\gamma(u_1u_2,\varepsilon)\gamma(\varepsilon,v_1v_2)).\end{aligned}$$

Noting that $|u_1u_2| = n \Leftrightarrow |v_1v_2| = n$, then we have all possible cases. Hence (R4) holds in $\Pi(\varphi,\psi)$ as claimed. ☐

We now use Lemmas 3.6 and 3.7 alongside Theorem 3.4 to prove Theorem 3.5.

Proof of Theorem 3.5 By Theorem 3.4, if $\Pi(\varphi,\psi)$ is finitely generated then $|A|, |B| < \infty$, $F = \mathrm{Gp}\langle x : x^n = 1\rangle$ for some $n \in \mathbb{N}$, and $\varphi(A) = \{x^p\}$, $\psi(B) = \{x^q\}$ for some $1 \le p, q \le n$ with $\gcd(p,n) = \gcd(q,n) = 1$. Let

$$\bar{\Gamma} := \{\gamma(u,v) : u \in A^*, v \in B^*,\ p|u| \equiv q|v| \bmod n,\ 0 \le |u|, |v| \le n\}$$

and

$$\Gamma := \bar{\Gamma} \setminus \{\gamma(u,v) : u \in A^*, v \in B^*, |u| = |v| = n \text{or } |u| = |v| = 0\}$$

be sets of formal symbols. Let R be the set of relations on Γ given by (R1)–(R4) in Lemmas 3.6 and 3.7. Let $\bar{\pi} : \Gamma \to \Pi(\varphi, \psi)$ be given by $\bar{\pi}(\gamma(u,v)) = (u,v)$, and let $\pi : \Gamma^* \to \Pi(\varphi, \psi)$ be the unique homomorphism extending $\bar{\pi}$. We will show that $\Pi(\varphi, \psi) \cong \mathrm{Mon}\langle \Gamma : R \rangle$ by the first isomorphism theorem, by showing $\ker \pi = R^\sharp$ (where $R^\sharp$ is the smallest congruence on Γ^* containing R) and noting that π is surjective.

By Lemma 3.6 and 3.7, it follows that $\ker \pi \supseteq R$, and hence $\ker \pi \supseteq R^\sharp$.

To show that $\ker \pi \subseteq R^\sharp$, we make the following claims:

Claim 1: For all $w \in \Gamma^*$,

$$\begin{aligned}(w, w_1 w_2 w_3) \in R^\sharp \text{ for some } w_1 &\in \{\gamma(u,v) \in \Gamma : 0 < |u|, |v| < n\} \cup \{\varepsilon_\Gamma\}, \\ w_2 &\in \{\gamma(u,v) \in \Gamma : |u| = n\}^*, \\ w_3 &\in \{\gamma(u,v) \in \Gamma : |v| = n\}^*,\end{aligned} \tag{2}$$

where ε_Γ denoted the empty word over the alphabet Γ.

Claim 2: For all $w, w' \in \Gamma^*$, if $(w, w') \in \ker \pi$, then $(w, z), (w', z) \in R^\sharp$ for some $z \in \Gamma^*$.

By transitivity, it follows from Claim 2 that if $(w, w') \in \ker \pi$, then $(w, w') \in R^\sharp$ also, and hence $\ker \pi \subseteq R^\sharp$. We will then have shown $\ker \pi = R^\sharp$, and

$$\Pi(\varphi, \psi) \cong \Gamma^*/\ker \pi = \Gamma^*/R^\sharp = \mathrm{Mon}\langle \Gamma : R \rangle,$$

giving a finitely presentation for $\Pi(\varphi, \psi)$, proving the theorem. It thus remains to prove Claims 1 and 2.

Proof of Claim 1: Again we note that for $\gamma(u,v) \in \Gamma$, $|u| = n$ if and only if $|v| = 0$, and similarly $|u| = 0$ if and only if $|v| = n$. We briefly adopt some terminology for letters in Γ to this end. We will say that $\gamma(u,v) \in \Gamma$ is of ε-type if either $u = \varepsilon$ or $v = \varepsilon$. Otherwise, $\gamma(u,v)$ will be of ϕ-type. The following rewriting procedure on w proves the claim:

(A1) If a letter of ϕ-type in w is preceded by a letter of ε-type, then (R2) and (R3) allows us to replace them with a letter of ϕ-type followed by a letter of ε-type. Hence using a sequence of (R2) and (R3) allows us to rewrite w as $w'w''$, where w' is a (possibly empty) word consisting of ϕ-type letters, and w'' is a (possibly empty) word consisting of ε-type letters. That is, $(w, w'w'') \in R^\sharp$ for some $w' \in \{\gamma(u,v) \in \Gamma : 0 < |u|, |v| < n\}^*$, $w'' \in \{\gamma(u,v) \in \Gamma : u = \varepsilon \text{ or } v = \varepsilon\}^*$.

(A2) As (R4) allows us to replace two concurrent ϕ-type letters with at most one ϕ-type letter followed by at most two ε-type letters, then repeatedly using (R4) from right to left on the letters in w' allows us to rewrite $w'w''$ as $w_1 w'''$ for w_1 a ϕ-type letter (or the empty word), and w''' a (potentially empty) word consisting of ε-type letters. That is, $(w'w'', w_1 w''') \in R^\sharp$ for some $w_1' \in \{\gamma(u,v) \in \Gamma : 0 < |u|, |v| < n\} \cup \{\varepsilon_\Gamma\}$, $w''' \in \{\gamma(u,v) \in \Gamma : u = \varepsilon \text{ or } v = \varepsilon\}^*$.

(A3) As (R1) allows us to swap the order of any two concurrent ε-type letters, then repeatedly using (R1) on the letters of w''' allows us to rewrite w''' as w_2w_3, where $w_2 \in \{\gamma(u,v) \in \Gamma : |u| = n\}^*$, $w_3 \in \{\gamma(u,v) \in \Gamma : |v| = n\}^*$. That is $(w_1w''', w_1w_2w_3) \in R^\sharp$ where w_1, w_2, w_3 are as in (2). Hence $(w, w_1w_2w_3) \in R^\sharp$ as claimed.

Proof of Claim 2: Let $w, w' \in \Gamma^*$ be such that $(w, w') \in \ker\pi$. Note by Claim 1,

$$(w, w_1w_2w_3), (w', w_1'w_2'w_3') \in R^\sharp \text{ for some } \begin{array}{l} w_1, w_1' \in \{\gamma(u,v) \in \Gamma : 0 < |u|, |v| < n\} \cup \{\varepsilon_\Gamma\}, \\ w_2, w_2' \in \{\gamma(u,v) \in \Gamma : |u| = n\}^*, \\ w_3, w_3' \in \{\gamma(u,v) \in \Gamma : |v| = n\}^*. \end{array}$$

As $R^\sharp \subseteq \ker\pi$, then $(w, w_1w_2w_3), (w', w_1'w_2'w_3') \in \ker\pi$ also. By assumption of $(w, w') \in \ker\pi$, it also follows that $(w_1w_2w_3, w_1'w_2'w_3') \in \ker\pi$ also. We will further show that $w_1 = w_1'$, $w_2 = w_2'$, $w_3 = w_3'$, so that taking $z = w_1w_2w_3$ proves the claim.

Firstly, consider for a contradiction that $w_1 \neq w_1'$. Then as $w_1, w_1' \in \{\gamma(u,v) \in \Gamma : 0 < |u|, |v| < n\} \cup \{\varepsilon_\Gamma\}$, then $w_1 = \gamma(u,v)$, $w_1' = \gamma(u',v')$, where either $u \neq u'$ or $v \neq v'$.

If $u \neq u'$, then if $|u| = |u'|$, it follows that $\pi(w) \neq \pi(w')$, as $\pi(w_1) = (u,v)$ and $\pi(w_1') = (u',v')$ are non-equal prefixes of $\pi(w)$ and $\pi(w')$ respectively, contradicting $(w, w') \in \ker\pi$.

Otherwise, if $|u| \neq |u'|$, then $\pi(w) \neq \pi(w')$, as the first coordinates in $\pi(w)$ and $\pi(w')$ are words in A^*, whose lengths are congruent to $|u|$ and $|u'|$ modulo n, respectively.

The argument for the case where $v \neq v'$ is the same as for $u \neq u'$. Hence $\pi(w) \neq \pi(w')$ if $w_1 \neq w_1'$, and so it must be that $w_1 = w_1'$ to avoid contradiction.

Let $\pi(w_1) = \pi(w_1') = (u_1, v_1)$. As $w_2, w_2' \in \{\gamma(u,v) \in \Gamma : |u| = n\}^*$, it follows that $\pi(w_2) = (u, \varepsilon)$ and $\pi(w_2') = (u', \varepsilon)$ for some $u, u' \in A^*$ (again noting that for $\gamma(u,v) \in \Gamma, |u| = n$ if and only if $|v| = 0$). Dually, $\pi(w_3) = (\varepsilon, v)$, $\pi(w_3') = (\varepsilon, v')$ for some $v, v' \in B^*$. Thus $\pi(w_1w_2w_3) = (u_1u, v_1v)$, and $\pi(w_1'w_2'w_3') = (u_1u', v_1v')$. As $(w_1w_2w_3, w_1'w_2'w_3') \in \ker\pi$, then $u_1u = u_1u'$, $v_1v = v_1v'$, and hence $u = u'$ and $v = v'$.

It follows that $\pi(w_2) = \pi(w_2')$ and $\pi(w_3) = \pi(w_3')$. Thus as π is injective on $\{\gamma(u,v) \in \Gamma : |u| = n\}^*$ and on $\{\gamma(u,v) \in \Gamma : |v| = n\}$, we have $w_2 = w_2'$ and $w_3 = w_3'$. This ends the proof of Claim 2, and hence also of the theorem by the earlier argument that the claims are sufficient. $\square$

4 Infinite fiber quotients

From the results of the above section, one might expect that infinite fiber quotients would give rise to many more finitely generated fiber products of free semigroups and free monoids. We thus seek to classify some properties of fiber quotients which give finitely generated fiber products. In this section, we obtain some necessary semigroup theoretic conditions for finite generation in the general infinite fiber quotient case. We begin with observation that the quotient itself must at least be finitely generated.

Lemma 4.1 *Let S, T, F be semigroups, and let $\varphi : S \to F$, $\psi : T \to F$ be epimorphisms. If $\Pi(\varphi, \psi)$ is finitely generated, then S, T and F are finitely generated.*

Proof Suppose that $\Pi(\varphi, \psi)$ is finitely generated, and let

$$V := \{(s_i, t_i) : 1 \leq i \leq n\} \subseteq \Pi(\varphi, \psi)$$

be a generating set for $\Pi(\varphi, \psi)$. Then $\pi_1(V) = \{s_i : 1 \leq i \leq n\}$ generates S (as $\Pi(\varphi, \psi)$ is subdirect), $\pi_2(V) = \{t_i : 1 \leq i \leq n\}$ generates T, and as φ is a surjection, it follows that $\varphi(\pi_1(V))$ is a generating set for F. $\square$

We also note in the next two results that finite generation of a fiber product of two free semigroups/monoids is equivalent to the fiber product having finitely many indecomposable elements.

Lemma 4.2 *Let F be a semigroup, and let $\varphi : A^+ \to F$, $\psi : B^+ \to F$ be two epimorphisms with A, B alphabets. Then $\Pi(\varphi, \psi)$ is finitely generated if and only if $\Pi(\varphi, \psi)$ has finitely many indecomposable elements.*

Proof As every generating set for $\Pi(\varphi, \psi)$ contains the set of indecomposable elements, sufficiency is immediate.

For necessity, we show that the set of indecomposable elements generates $\Pi(\varphi, \psi)$. Let $(u, v) \in \Pi(\varphi, \psi)$. If (u, v) is indecomposable, then there is nothing to show. Otherwise, if $(u, v) \in \Pi(\varphi, \psi)^2$, then there exist $(u', v'), (u'', v'') \in \Pi(\varphi, \psi)$ with $(u, v) = (u', v')(u'', v'')$. As $u \in A^+$, $v \in B^+$, it follows that $|u'|, |u''| < |u|$ and $|v'|, |v''| < |v|$.

Repeating this factoring process on (u', v') or (u'', v'') if either are decomposable, and so on with their decomposable factors, then as the lengths of the words in the factors of (u, v) decrease in every factorisation, it follows that this process is finite. Hence

$$(u, v) = (u_1, v_1)(u_2, v_2) \dots (u_n, v_n)$$

where (u_i, v_i) are indecomposable for $1 \leq i \leq n$, and $n \leq \min\{|u|, |v|\}$. Thus (u, v) is generated by indecomposable elements and thus $\Pi(\varphi, \psi)$ is finitely generated, and so the result follows. $\square$

Lemma 4.3 *Let F be a monoid, and let $\varphi : A^* \to F$, $\psi : B^* \to F$ be two epimorphisms with A, B alphabets. Then $\Pi(\varphi, \psi)$ is finitely generated if and only if $\Pi(\varphi, \psi)$ has finitely many indecomposable elements.*

Proof Similarly to Lemma 4.2, sufficiency is immediate, and we argue for necessity that the monoid indecomposable elements of $\Pi(\varphi, \psi)$ are a generating set by expressing every element of $\Pi(\varphi, \psi)$ as a product of indecomposables.

If $(u, v) \in \Pi(\varphi, \psi)$ is indecomposable in the monoid sense, then (u, v) is a product of indecomposable elements and there is nothing to show. Otherwise, (u, v) is decomposable as a product

$$(u, v) = (u', v')(u'', v'')$$

where either $|u'| < |u|$ or $|u''| < |u|$, and also $|v'| < |v|$ or $|v''| < |v|$. We can repeat the factoring process on either (u', v') or (u'', v'') similarly to Lemma 4.2 if either are decomposable.

As (u, v) is such that either $u \in A^+$ or $v \in B^+$ (noting that the singleton exception $(\varepsilon, \varepsilon)$ can be included in any generating set without changing its cardinality), and $u \in A^+$ (resp. $v \in B^+$) is decomposable into at most $|u|$ factors in A^+ (resp. $|v|$ factors in B^+), it follows that in this factoring process, (u, v) can be decomposed into a product of at most $|u| + |v|$ elements of $\Pi(\varphi, \psi) \setminus \{(\varepsilon, \varepsilon)\}$, each of which must be an indecomposable element. This concludes the proof. $\square$

Our next result shows that no finitely generated fiber product of two free semigroups can have a fiber quotient containing a finite subsemigroup.

Proposition 4.4 *Let $\varphi : A^+ \to S$, $\psi : B^+ \to S$ be two epimorphisms onto a semigroup S. If the fiber product of A^+ with B^+ over S with respect to φ, ψ is finitely generated, then S is idempotent-free.*

Proof Suppose to the contrary, that $e^2 = e$ for some $e \in S$. Then by surjectivity, there exists $u \in A^+, v \in B^+$ such that $\varphi(u) = e = \psi(v)$. Then for all $n \in \mathbb{N}$, as $\psi(v^n) = e^n = e$, it follows that $(u, v^n) \in \Pi(\varphi, \psi)$.

If $X = \{(u_i, v_i) : 1 \le i \le p\} \subseteq A^+ \times B^+$ were a finite generating set for $\Pi(\varphi, \psi)$, then as u can be decomposed into at most $|u|$ factors in A^+, it follows that each pair (u, v^n) can be decomposed into at most $|u|$ factors in $\langle X \rangle$. This is a contradiction, as this implies that $|v^n| \le |u| \max_{1 \le i \le p} |v_i|$ for all $n \in \mathbb{N}$. $\square$

Our next result tells us about Green's relations on fiber quotients of fiber products of free semigroups, and in particular that they are all equal to the trivial relation.

Proposition 4.5 *Let $\varphi : A^+ \to S$, $\psi : B^+ \to S$ be two epimorphisms onto a semigroup S. If the fiber product of A^+ with B^+ over S with respect to φ, ψ is finitely generated, then S is $\mathcal{J}$-trivial.*

Proof Suppose to the contrary, that there exist some $s, t \in S$ with $(s, t) \in \mathcal{J}$, but $s \neq t$. Then in particular, there exist $x, y, x', y' \in S^1$ such that $s = xty$, $t = x'sy'$. In particular, $s = (xx')^n s (y'y)^n$ for all $n \in \mathbb{N}$.

If S is a monoid, then it has an idempotent, and hence $\Pi(\varphi, \psi)$ is not finitely generated by Proposition 4.4. Hence we assume that S is not a monoid, and hence $S^1 = S \cup \{1\}$, where 1 is an identity symbol adjoined to S.

As $s \neq t$ by assumption, it follows that at most one of x and y can equal 1, and similarly at most one of x' and y' can equal 1. It follows that at most one of xx' and

$y'y$ can equal 1, for otherwise $x = x' = y = y' = 1$. That is, at least one of xx' or $y'y$ is an element of S. We consider the possible cases of when either $xx' \in S$ or $y'y \in S$.

If $xx' \in S$ and $y'y \in S$, then by surjectivity, there exists $u \in A^+$ and $v, w, w' \in B^+$ such that $\varphi(u) = s$, $\psi(v) = s$, $\psi(w) = xx'$, and $\psi(w') = y'y$. Hence $(u, w^n v(w')^n) \in \Pi(\varphi, \psi)$ for all $n \in \mathbb{N}$. If $X = \{(u_i, v_i) : 1 \le i \le p\} \subseteq A^+ \times B^+$ were a finite generating set for $\Pi(\varphi, \psi)$, then as u can be decomposed into at most $|u|$ factors in A^+, it follows that each pair $(u, w^n v(w')^n)$ can be decomposed into at most $|u|$ factors in $\langle X \rangle$. This is a contradiction, as this implies that $|w^n v(w')^n| \le |u| \max_{1 \le i \le p} |v_i|$ for all $n \in \mathbb{N}$.

If $xx' \in S$, but $y'y \notin S$, then $s = (xx')^n s$ for all $n \in \mathbb{N}$, and by surjectivity, there exists $u \in A^+$ and $v, w \in B^+$ such that $\varphi(u) = s$, $\psi(v) = s$, and $\psi(w) = xx'$. Hence $(u, w^n v) \in \Pi(\varphi, \psi)$ for all $n \in \mathbb{N}$. A similar contradiction to the case where $xx', y'y \in S$ can be obtained supposing there were a finite generating set for $\Pi(\varphi, \psi)$.

The last case, $xx' \notin S$ but $y'y \in S$, is similar to the previous case. Hence in all cases, there can be no finite generating set for $\Pi(\varphi, \psi)$. This concludes the proof by contrapositive. □

In the next result, we show that the properties of being $\mathcal{J}$-trivial and idempotent-free are not sufficient conditions for finite generation of fiber products of free semigroups. We draw an analogy with Theorem 3.4 by choosing the free monogenic semigroup as a fiber, and show in particular that conditions on the associated homomorphisms are again necessary.

Theorem 4.6 *Let A^+, B^+ be two free semigroups with A,B finite, and let $\varphi : A^+ \to \mathbb{N}$, $\psi : B^+ \to \mathbb{N}$ be two epimorphisms, where $\mathbb{N}$ is considered with addition. Then the fiber product $\Pi(\varphi, \psi)$ of A^+ with B^+ over $\mathbb{N}$ with respect to φ, ψ is finitely generated if and only if either $|\varphi(A)| = 1$ or $|\psi(B)| = 1$.*

Proof ($\Rightarrow$) We show the contrapositive. If $|\varphi(A)|, |\psi(B)| > 1$, then assume without loss that there exists $a \in A, b \in B$ such that $\varphi(a) = m, \psi(b) = n$, for some $m \ge n > 1$. As φ is surjective, there exists some $x \in A$, $y \in B$ such that $\varphi(x) = 1 = \psi(y)$. Note that $m = qn + r$ for some $q \in \mathbb{N}$, $0 \le r < n$. As $\varphi(xa^k) = 1 + km = \psi((b^q y^r)^k y)$ (where y^0 is taken to be the empty word), it follows that $(xa^k, (b^q y^r)^k y) \in \Pi(\varphi, \psi)$ for all $k \in \mathbb{N}$.

We claim that $(xa^k, (b^q y^r)^k y)$ is irreducible in $\Pi(\varphi, \psi)$, for all $k \in \mathbb{N}$. For otherwise, $(xa^k, (b^q y^r)^k y) = (u, v)(u', v')$ for some $u, u' \in A^+$, $v, v' \in B^+$, where u and v are proper prefixes of xa^k and $(b^q y^r)^k y$ respectively. Any proper prefix u of xa^k is such that $\varphi(u) \equiv 1 \pmod{m}$, but any proper prefix v of $(b^q y^r)^k y$ is such that $\psi(v) \equiv j \pmod{m}$, where $j \in \{0, n, 2n, \dots, qn, qn + 1, qn + 2, \dots, qn + r - 1\}$.

As $n \ne 1$ by assumption, and k comes from a subset of least positive residues modulo m, it follows that $\psi(v) \not\equiv 1 \pmod{m}$, contradicting that $(u, v) \in \Pi(\varphi, \psi)$. This proves the claim, and hence as any generating set for $\Pi(\varphi, \psi)$ must contain $\{(xa^k, (b^q y^r)^k y) : k \in \mathbb{N}\}$, it follows that $\Pi(\varphi, \psi)$ is not finitely generated.

($\Leftarrow$) It is enough to prove the statement assuming $|\varphi(A)| = 1$ without loss. As this is equivalent to $\varphi(a) = 1$ for all $a \in A$ by surjectivity of φ, it follows that

$$\Pi(\varphi, \psi) = \{(u, v) \in A^+ \times B^+ \,:\, |u| = \psi(v)\}.$$

We claim that $\Pi(\varphi, \psi)$ is generated by the set

$$X = \{(u, v) \in A^+ \times B^+ \,:\, v \in B, |u| = \psi(v)\}$$

which is finite, as B is finite.

Clearly $\langle X \rangle \subseteq \Pi(\varphi, \psi)$. To prove the opposite containment, let $(u, v) \in \Pi(\varphi, \psi)$. Then as $u = a_1 a_2 \dots a_{|u|}$ for some $a_1, \dots, a_{|u|} \in A$, and $v = b_1 b_2 \dots b_{|v|}$ for some $b_1, \dots, b_{|v|} \in B$, it follows that $|u| = \psi(v) = \sum_{i=1}^{|v|} \psi(b_i)$. As

$$(u, v) = (a_1 a_2 \dots a_{|u|}, b_1 b_2 \dots b_{|v|}) = \prod_{i=0}^{|v|-1} (a_{j_i+1} a_{j_i+2} \dots a_{j_i+\psi(b_{i+1})}, b_{i+1}) \in \langle X \rangle \quad (3)$$

where

$$j_i = \begin{cases} 0 & \text{if } i = 0 \\ \psi(b_1 b_2 \dots b_i) & \text{otherwise,} \end{cases}$$

the claim holds, as (3) gives a decomposition of (u, v) into a product of elements in X. ☐

Our next example notes that the above result does not, however, generalise to the class of free commutative semigroups.

Example 4.7 Let A^+, B^+ be two free semigroups, and let $\varphi : A^+ \to F$, $\psi : B^+ \to F$ be two epimorphisms onto a free commutative semigroup F of (finite) rank larger than one. Then the fiber product of A^+ with B^+ over F with respect to φ, ψ is not finitely generated.

Proof Let $x, y \in F$ be two distinct generators for F. Then as φ, ψ are surjections, there exist $a, a' \in A$, $b, b' \in B$ such that $\varphi(a) = \psi(b) = x$, and $\varphi(a') = \psi(b') = y$. As F is commutative, then $x^n y = y x^n$ for all $n \in \mathbb{N}$, and so it follows that $(a^n a', b' b^n) \in \Pi(\varphi, \psi)$ for all $n \in \mathbb{N}$.

As any proper prefix u of $a^n a'$ is a power of a, it follows that $\varphi(u)$ is a power of x. But as any proper prefix v of $b' b^n$ begins with b', it follows that $\psi(v)$ contains a y. Hence $(a^n a', b' b^n)$ is indecomposable in $\Pi(\varphi, \psi)$ for all $n \in \mathbb{N}$, as there are no proper prefixes u of $a^n a'$, v of $b' b^n$ such that $(u, v) \in \Pi(\varphi, \psi)$. ☐

5 Decision problems for free quotients

Perhaps the most natural example of semigroups satisfying the necessary conditions of finite generation given above in Lemma 4.1, Propositions 4.4, and 4.5 are the finitely generated free semigroups and monoids. Hence in this section, we consider some decision problems for fiber products of free semigroups/monoids with free fiber quotients. Our first observation establishes an equivalence between word problems in the fiber product and fiber quotient.

Lemma 5.1 *Let S, T, F be semigroups, and let $\varphi : S \to F$, $\psi : T \to F$ be epimorphisms, with $\Pi(\varphi, \psi)$ finitely generated. Then the generalized word problem for $\Pi(\varphi, \psi)$ in $S \times T$ is decidable if and only if the word problem of F is decidable.*

Proof Let $X \subseteq S \times T$ be any generating set for $S \times T$, w be a word over X, and $\pi : X^+ \to S \times T$ be the natural homomorphism. Then $\pi(w) \in \Pi(\varphi, \psi)$ if and only if $\varphi(\pi_S(\pi(w))) = \psi(\pi_T(\pi(w)))$. As F is finitely generated by Lemma 4.1, then by writing $\varphi(\pi_S(\pi(w)))$ and $\psi(\pi_T(\pi(w)))$ as words over any finite generating set Y, it is decidable whether or not $(\varphi(\pi_S(\pi(w))), \psi(\pi_T(\pi(w))) \in \mathrm{WP}(F, Y)$ and hence whether or not w represents a word in $\Pi(\varphi, \psi)$. Hence the generalized word problem for $\Pi(\varphi, \psi)$ in $S \times T$ is decidable.

For the reverse direction, let $Y \subseteq F$ be any finite generating set for F (whose existence is given by Lemma 4.1), u, v be words over Y, and $\pi : Y^+ \to F$ be the natural homomorphism. Given a finite generating set X for $S \times T$, the images $\pi_S(X)$ and $\pi_T(X)$ are finite generating sets for S and T respectively. As φ, ψ are surjections, then there exists $(s, t) \in S \times T$ such that $(\varphi(s), \psi(t)) = (\pi(u), \pi(v))$. In particular, such an s and t can be found in finite time by enumerating all products in S over $\pi_S(X)$ up to length $|u|$, and all products in S over $\pi_T(X)$ up to length $|v|$ respectively. Considering $(s,\ t)$ as a product of elements of X, it is decidable whether or not $(s,\ t)$ represents a word in $\Pi(\varphi, \psi)$ by decidability of the generalized word problem for $\Pi(\varphi, \psi)$ in $S \times T$, and hence whether or not $(u, v) \in \mathrm{WP}(F, Y)$. Hence the word problem of F is decidable.

For the remainder of this section, we seek to answer the following decision question:

Question 5.2 Is the finite generation problem for a fiber product of two free monoids with a free monoid fiber quotient decidable?

To answer this, we use a two tape automaton construction, for which we use the following definition:

Definition 5.3 A *two-tape automaton* is a 6-tuple $\mathcal{A} = (Q, \Sigma_1, \Sigma_2, \delta, \iota, F)$, where Q is a finite set of states, Σ_1, Σ_2 are two input alphabets, $\delta \subseteq Q \times \Sigma \times Q$ is the transition relation (where $\Sigma = (\Sigma_1 \cup \{\varepsilon_1\}) \times (\Sigma_2 \cup \{\varepsilon_2\})$, and $\varepsilon_1, \varepsilon_2$ are the empty words over Σ_1, Σ_2 respectively), $\iota \in Q$ is the initial state, $F \subseteq Q$ is the set of final states.

An *input* is a pair of words $(u, v) \in \Sigma_1^* \times \Sigma_2^*$. A two-tape automaton $\mathcal{A}$ *accepts the input* $(u,\ v)$ if there exists a finite sequence of transitions $(q_{i-1}, \sigma_i, q_i)_{i=1}^k$ where $q_0 = \iota$, $q_k \in F$, and $(u, v) = \sigma_i \dots \sigma_k$. The *language accepted by* $\mathcal{A}$ is the set $\mathcal{L}(\mathcal{A})$ of all inputs accepted by $\mathcal{A}$.

Finally, a *cycle* of a two-tape automaton is a finite sequence of transitions $(q_{i-1}, \sigma_i, q_i)_{i=1}^k$ where $q_0 = q_k$.

The construction process used in answering Question 5.2 is then as follows. Let $\varphi : A^* \to C^*$, $\psi : B^* \to C^*$ be two epimorphisms with A, B, C finite alphabets. We will denote by $\varepsilon_A, \varepsilon_C$ and ε_C the empty words in A^*, B^* and C^* respectively. Let $\mathcal{A}_{\varphi,\psi} = (Q, \Sigma_1, \Sigma_2, \delta, \iota, F)$ be the associated two tape automaton (where an input $(u, v) \in A^* \times B^*$) given by the following:

- $Q := Q_1 \cup Q_2 \cup \{\iota\} \cup \{(\varepsilon_C, \varepsilon_C)\}$ where
$$Q_1 := \{(u, \varepsilon_C) \in C^+ \times \{\varepsilon_C\} : (\exists w \in \varphi(A))(u <_s w)\};$$
$$Q_2 := \{(\varepsilon_C, v) \in \{\varepsilon_C\} \times C^+ : (\exists w \in \psi(B))(v <_s w)\};$$
- $\Sigma_1 := A, \Sigma_2 := B$.
- $\delta = \bigcup_{i=1}^{8} \Delta_i \subseteq Q \times \Sigma \times Q$, where
$$\Delta_1 = \{(\iota, (a, \varepsilon_B), (\varepsilon_C, \varepsilon_C)) : a \in A, \varphi(a) = \varepsilon_C\}$$
$$\Delta_2 = \{(\iota, (\varepsilon_A, b), (\varepsilon_C, \varepsilon_C)) : b \in B, \psi(b) = \varepsilon_C\}$$
$$\Delta_3 = \{(\iota, (a, b), (\psi(b)^{-1}\varphi(a), \varepsilon_C)) : a \in A, b \in B, \psi(b) \leq_p \varphi(a), \psi(b) \neq \varepsilon_C\};$$
$$\Delta_4 = \{(\iota, (a, b), (\varepsilon_C, \varphi(a)^{-1}\psi(b)) : a \in A, b \in B, \varphi(a) \leq_p \psi(b), \varphi(a) \neq \varepsilon_C\};$$
$$\Delta_5 = \{((u, \varepsilon_C), (\varepsilon_A, b), (\psi(b)^{-1}u, \varepsilon_C)) : b \in B, u \neq \varepsilon_C,\ \psi(b) \leq_p u\};$$
$$\Delta_6 = \{((u, \varepsilon_C), (\varepsilon_A, b), (\varepsilon_C, u^{-1}\psi(b))) : b \in B, u \neq \varepsilon_C,\ u \leq_p \psi(b)\};$$
$$\Delta_7 = \{((\varepsilon_C, v), (a, \varepsilon_B), (\varepsilon_C, \varphi(a)^{-1}v)) : a \in A, v \neq \varepsilon_C,\ \varphi(a) \leq_p v\};$$
$$\Delta_8 = \{((\varepsilon_C, v), (a, \varepsilon_B), (v^{-1}\varphi(a), \varepsilon_C) : a \in A, v \neq \varepsilon_C,\ v \leq_p \varphi(a)\};$$
- ι is the initial state, $F = \{(\varepsilon_C, \varepsilon_C)\}$ is the set of final states.

Example 5.4 Let $\varphi : \{a, b\}^* \to \{x\}^*$ be defined by $\varphi(a) = \varphi(b) = x$, and let $\psi : \{a, b\}^* \to \{x\}^*$ be defined by $\varphi(a) = x^3$, $\psi(b) = x^2$. Then $\varphi(\{a, b\}) = \{x\}$ which contains no words with proper suffixes, and hence $Q_1 = \emptyset$. However, $\psi(\{a, b\}) = \{x^2, x^3\}$, for which the set of proper suffixes is $\{x, x^2\}$. Hence $Q_2 = \{(\varepsilon_C, x), (\varepsilon_C, x^2)\}$. Thus $\mathcal{A}_{\varphi,\psi}$ has state set

$$Q = \{\iota, (\varepsilon_C, x), (\varepsilon_C, x^2), (\varepsilon_C, \varepsilon_C)\}.$$

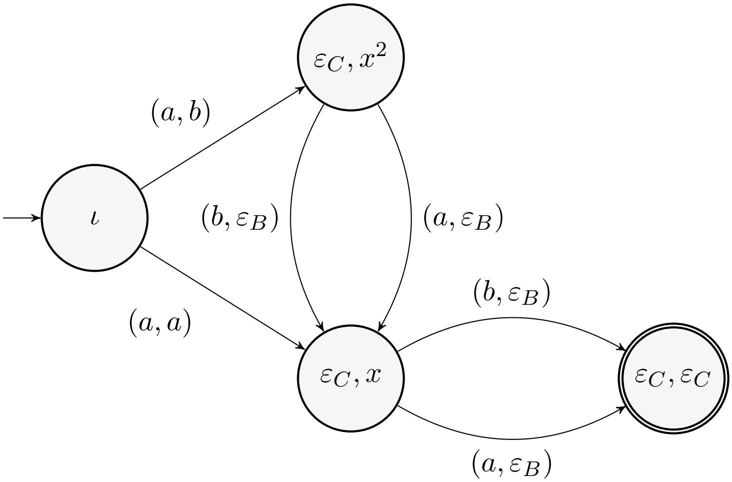
For the edges in δ, we note that $\Delta_1 = \Delta_2 = \emptyset$, as $\varepsilon_C \notin \varphi(\{a, b\})$ and $\varepsilon_C \notin \psi(\{a, b\})$. Δ_3 is also empty, as $\varphi(\{a, b\}) = \{x\}$, for which the only prefixes are ε_C and x, which are not in $\psi(\{a, b\})$.

For Δ_4 however, we obtain the edges $(\iota, (a, a), (\varepsilon_C, x))$ (as $\varphi(a) = x, \psi(a) = x^2$, and $\varphi(a) \leq_p \psi(a)$ with $\varphi(a)^{-1}\psi(a) = x^{-1}x^2 = x$) and $(\iota, (a, b), (\varepsilon_C, x^2))$ (as $\varphi(a) = x, \psi(b) = x^3$, and $\varphi(a) \leq_p \psi(b)$ with $\varphi(a)^{-1}\psi(b) = x^{-1}x^3 = x^2$).

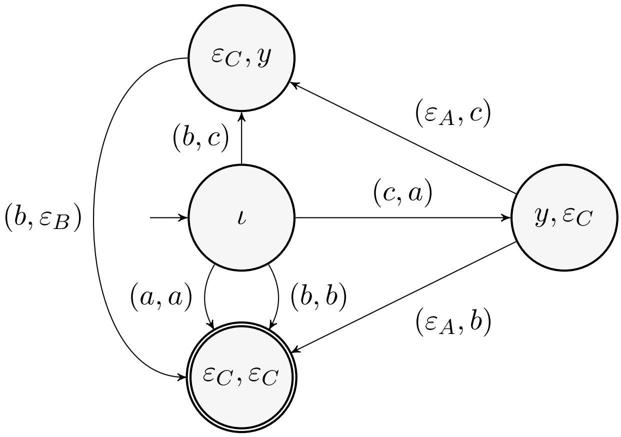
Δ_5 and Δ_6 are empty once more, as there are no states of the form $(u, \varepsilon_C) \in Q_1$ as Q_1 is empty. A verification similar to previous calculations however gives the edges

$$((\varepsilon_C, x^2), (b, \varepsilon_B), (\varepsilon_C, x)), \qquad ((\varepsilon_C, x^2), (a, \varepsilon_B), (\varepsilon_C, x)),$$
$$((\varepsilon_C, x), (b, \varepsilon_B), (\varepsilon_C, \varepsilon_C)), \qquad ((\varepsilon_C, x), (a, \varepsilon_B), (\varepsilon_C, \varepsilon_C))$$

from Δ_7. Noting that $\Delta_8 = \emptyset$, we obtain the full automaton $\mathcal{A}_{\varphi,\psi}$, as seen below.



Example 5.5 Let $\varphi : \{a, b, c\}^* \to \{x, y\}^*$, $\psi : \{a, b, c\}^* \to \{x, y\}^*$ be defined by $\varphi(a) = x, \varphi(b) = y, \varphi(c) = xy$ and $\psi(a) = x, \psi(b) = y, \psi(c) = y^2$. Then $\mathcal{A}'$ is given below.



We utilise this automatic construction in the following result.

Theorem 5.6 *Let $\varphi : A^* \to C^*$, $\psi : B^* \to C^*$ be two epimorphisms with A, B, C finite alphabets, and let $\mathcal{A}_{\varphi,\psi}$ be the associated automaton given as above. Then the* *fiber product of A^* with B^* over C^* with respect to φ, ψ is finitely generated if and only if $\mathcal{A}_{\varphi,\psi}$ has no cycles.*

In order to prove this result, we utilise the following lemmas.

Lemma 5.7 *Let $(u, v) \in Q$, and let $(\alpha, \beta) \in A^* \times B^*$. If a path from ι to (u, v) has label (α, β), then*

$$\varphi(\alpha)v = \psi(\beta)u. \tag{4}$$

Proof We proceed by induction on path length. The paths of length one are precisely the transitions $p \in \Delta_1 \cup \Delta_2 \cup \Delta_3 \cup \Delta_4$. For $p \in \Delta_1 \cup \Delta_2$, (4) holds by definition . If $p \in \Delta_3$, then $p = (\iota, (a, b), (\psi(b)^{-1}\varphi(a), \varepsilon_C))$ for some $a \in A, b \in B$, and

$$\varphi(\alpha)v = \varphi(a) = \psi(b)\psi(b)^{-1}\varphi(a) = \psi(\beta)u$$

as required. Similarly if $p \in \Delta_4$, then $p = (\iota, (a, b), (\varepsilon_C, \varphi(a)^{-1}\psi(b)))$ for some $a \in A, b \in B$, and

$$\varphi(\alpha)v = \varphi(a)\varphi(a)^{-1}\psi(b) = \psi(b) = \psi(\beta)u.$$

As these are all the paths of length one, this proves the base case. For the inductive hypothesis, assume that if a path from ι to (u, v) of length k has label (α, β), then $\varphi(\alpha)v = \psi(\beta)u$.

Consider a path from ι to (u', v') of length $k + 1$ with label (α, β). Then necessarily there exists a path p of length k from ι to some state (u, v), and a transition p' from (u, v) to (u', v'). Then there are two cases for the label of p':

Case 1: If p' has label (ε_A, b) for some $b \in B$, then it follows that $v = \varepsilon_C$, and the path p has label $(\alpha, \beta b^{-1})$. If $\psi(b) \leq_p u$, then $(u', v') = (\psi(b)^{-1}u, \varepsilon_C)$ by the definition of Δ_5. Hence

$$\begin{aligned}\psi(\beta)u' &= \psi(\beta b^{-1})\psi(b)u' \\ &= \psi(\beta b^{-1})u \\ &= \varphi(\alpha)v \text{ by the inductive hypothesis} \\ &= \varphi(\alpha)v'.\end{aligned}$$

Otherwise, if $u \leq_p \psi(b)$, then $(u', v') = (\varepsilon_C, u^{-1}\psi(b))$ by the definition of Δ_6 . Hence

$$\begin{aligned}\psi(\beta)u' &= \psi(\beta b^{-1})\psi(b) \\ &= \psi(\beta b^{-1})uv' \\ &= \varphi(\alpha)vv' \text{ by the inductive hypothesis} \\ &= \varphi(\alpha)v'.\end{aligned}$$

Case 2: If p' has label (a, ε_B) for some $a \in A$, then it follows that $u = \varepsilon_C$, and the path p has label $(\alpha a^{-1}, \beta)$. If $\varphi(a) \leq_p v$, then $(u', v') = (\varepsilon_C, \varphi(a)^{-1}v)$ by the definition of Δ_7. Hence

$$\begin{aligned}\varphi(\alpha)v' &= \varphi(\alpha a^{-1})\varphi(a)v' \\ &= \varphi(\alpha a^{-1})v \\ &= \psi(\beta)u \text{ by the inductive hypothesis} \\ &= \psi(\beta)u'.\end{aligned}$$

Otherwise, if $v \leq_p \varphi(a)$, then $(u', v') = (v^{-1}\varphi(a), \varepsilon_C)$ by the definition of Δ_8. Hence

$$\begin{aligned}\varphi(\alpha)v' &= \varphi(\alpha a^{-1})\varphi(a) \\ &= \varphi(\alpha a^{-1})vu' \\ &= \psi(\beta)uu' \text{ by the inductive hypothesis} \\ &= \psi(\beta)u'.\end{aligned}$$

Thus the result holds by induction on paths of arbitrary length. □

Lemma 5.8 *Let $(\alpha, \beta) \in A^* \times B^*$. Then there is at most one path originating from ι with label (α, β) in $\mathcal{A}_{\varphi,\psi}$.*

Proof By definition of δ, the only paths originating from ι with label (α, β) for either $\alpha = \varepsilon_A$ or $\beta = \varepsilon_B$ are the length one transitions $p \in \Delta_1 \cup \Delta_2$, each of which is distinct.

Otherwise, any path p originating from ι with label $(\alpha, \beta) \in A^+ \times B^+$ is given by a sequence of transitions $(q_{i-1}, \sigma_i, q_i)_{i=1}^k$ such that $q_0 = \iota$ and $\sigma_1\sigma_2 \ldots \sigma_k = (\alpha, \beta)$. As $\alpha \in A^+$ and $\beta \in B^+$, then there exist unique decompositions $\alpha = a_1a_2 \ldots a_{|\alpha|}$ for some $a_1, \ldots, a_{|\alpha|} \in A$ and $\beta = b_1b_2 \ldots b_{|\beta|}$ for some $b_1, \ldots, b_{|\beta|} \in B$.

We claim that state q_{i-1} uniquely determines σ_i for $1 \leq i \leq k$. As p is a path in $\mathcal{A}_{\varphi,\psi}$, then $q_{i-1} \in \{\iota\} \cup Q_1 \cup Q_2$. By the definition of δ, the only instance where $q_{i-1} = \iota$ is when $i = 1$. Moreover, this implies that $\sigma_1 = (a_1, b_1)$, as $\sigma_1 \in A \times B$ and $\sigma_1\sigma_2 \ldots \sigma_k = (\alpha, \beta)$.

Further, as $q_{i-1} \in Q_2$ if and only if $\sigma_i \in A \times \{\varepsilon_B\}$, and as α has a unique decomposition over A, then $\sigma_i \in A \times \{\varepsilon_B\}$ if and only if $\sigma_i = (a_{j_i}, \varepsilon_B)$ where $j_i = |\pi_{A^*}(\sigma_1 \ldots \sigma_{i-1})| + 1$.

Finally as β has a unique decomposition over B, a similar proof shows $q_{i-1} \in Q_1 \Leftrightarrow \sigma_i = (\varepsilon_A, b_{k_i})$ where $k_i = |\pi_{B^*}(\sigma_1 \ldots \sigma_{i-1})| + 1$.

As $Q_1 \cap Q_2 \cap \{\iota\} = \emptyset$, then q_{i-1} uniquely determines σ_i, which together uniquely determine q_i by the definition of δ. Hence $q_0 = \iota$ and $(\alpha, \beta) = (a_1 \ldots a_{|\alpha|}, b_1 \ldots b_{|\beta|})$ uniquely determine the path p. □

Lemma 5.9 *Let $\varphi : A^* \to C^*, \psi : B^* \to C^*$ be two epimorphisms with A, B, C finite alphabets, let $\mathcal{A}_{\varphi,\psi}$ be the associated automaton given as above. Let $\Phi := \varphi \circ \pi_{A^*}$, and $\Psi := \psi \circ \pi_{B^*}$. Let $(q_{i-1}, \sigma_i, q_i)_{i=1}^k$ be a sequence of transitions with $q_0 = \iota$. Then either*

$$q_k = (\Psi(\sigma_1 \ldots \sigma_k)^{-1}\Phi(\sigma_1 \ldots \sigma_k), \varepsilon_C),$$

if $\Psi(\sigma_1 \ldots \sigma_k) \leq_p \Phi(\sigma_1 \ldots \sigma_k)$, or

$$q_k = (\varepsilon_C, \Phi(\sigma_1 \dots \sigma_k)^{-1}\Psi(\sigma_1 \dots \sigma_k))$$

if $\Phi(\sigma_1 \dots \sigma_k) \leq_p \Psi(\sigma_1 \dots \sigma_k)$.

Proof We proceed by induction on k. Firstly for the base case where $k = 1$, as $q_0 = \iota$, it follows that $(q_0, \sigma_1, q_1) \in \Delta_1 \cup \Delta_2 \cup \Delta_3 \cup \Delta_4$, from which the required form of q_1 follows by definition.

For the inductive hypothesis, assume that for $k = j$, we have either

$$q_j = (\Psi(\sigma_1 \dots \sigma_j)^{-1}\Phi(\sigma_1 \dots \sigma_j), \varepsilon_C), \tag{5}$$

or

$$q_j = (\varepsilon_C, \Phi(\sigma_1 \dots \sigma_j)^{-1}\Psi(\sigma_1 \dots \sigma_j)), \tag{6}$$

and consider the state q_{j+1} in the case where $q_j \neq (\varepsilon_C, \varepsilon_C)$. It suffices to assume only case (5), as the proof for case (6) will follow by a symmetric argument. As $\Psi(\sigma_1 \dots \sigma_j)^{-1}\Phi(\sigma_1 \dots \sigma_j) \neq \varepsilon_C$, by definition of Δ_5, Δ_6, it follows that $\sigma_{j+1} = (\varepsilon_A, b)$ for some $b \in B$, and either

$$\begin{aligned} q_{j+1} &= (\psi(b)^{-1}\Psi(\sigma_1 \dots \sigma_j)^{-1}\Phi(\sigma_1 \dots \sigma_j), \varepsilon_C) \\ &= ([\Psi(\sigma_1 \dots \sigma_j)\psi(b)]^{-1}\Phi(\sigma_1 \dots \sigma_j), \varepsilon_C) \\ &= ([\Psi(\sigma_1 \dots \sigma_j)\Psi(\sigma_{j+1})]^{-1}\Phi(\sigma_1 \dots \sigma_j), \varepsilon_C) \\ &= (\Psi(\sigma_1 \dots \sigma_{j+1})^{-1}\Phi(\sigma_1 \dots \sigma_{j+1}), \varepsilon_C), \end{aligned}$$

or

$$\begin{aligned} q_{j+1} &= (\varepsilon_C, [\Psi(\sigma_1 \dots \sigma_j)^{-1}\Phi(\sigma_1 \dots \sigma_j)]^{-1}\psi(b)) \\ &= (\varepsilon_C, \Phi(\sigma_1 \dots \sigma_j)^{-1}\Psi(\sigma_1 \dots \sigma_j)\psi(b)) \\ &= (\varepsilon_C, \Phi(\sigma_1 \dots \sigma_j)^{-1}\Psi(\sigma_1 \dots \sigma_j)\Psi(\sigma_{j+1})) \\ &= (\varepsilon_C, \Phi(\sigma_1 \dots \sigma_{j+1})^{-1}\Psi(\sigma_1 \dots \sigma_{j+1})) \end{aligned}$$

as expected. Hence the result follows by induction. □

Lemma 5.10 *Let $\varphi : A^* \to C^*$, $\psi : B^* \to C^*$ be two epimorphisms with A, B, C finite alphabets, and let $\mathcal{A}_{\varphi,\psi}$ be the associated automaton given as above. Then the language accepted by $\mathcal{A}_{\varphi,\psi}$ is the set of indecomposable elements of* $\Pi(\varphi, \psi)$.

Proof We first show that elements of $\mathcal{L}(\mathcal{A}_{\varphi,\psi})$ are indecomposable in $\Pi(\varphi, \psi)$. Let $(\alpha, \beta) \in \mathcal{L}(\mathcal{A}_{\varphi,\psi})$. Then there is a path $p = (q_{i-1}, \sigma_i, q_i)_{i=1}^k$ from ι to $(\varepsilon_C, \varepsilon_C)$ with label (α, β). By Lemma 5.8, it follows that $\varphi(\alpha) = \psi(\beta)$, and hence $(\alpha, \beta) \in \Pi(\varphi, \psi)$.

Further, suppose for a contradiction that (α, β) is decomposable. Then

$$(\alpha, \beta) = (\alpha', \beta')(\alpha'', \beta'') \tag{7}$$

for some $\alpha', \alpha'' \in A^*$, $\beta', \beta'' \in B^*$. To avoid contradiction, it must be that $\alpha \in A^+$ and $\beta \in B^+$, as the definition of δ' gives that the only pairs accepted by $\mathcal{A}_{\varphi,\psi}{}'$ involving ε_A or ε_B are those of the form $(\varepsilon_A, b), (a, \varepsilon_B)$ for $a \in A, b \in B$ with $\varphi(a) = \psi(b) = \varepsilon_C$ which are indecomposable in $\Pi(\varphi, \psi)$.

By the definition of δ', either $\sigma_1 = (\alpha_1, \varepsilon_B)$, $\sigma_1 = (\varepsilon_A, \beta_1)$ or $\sigma_1 = (\alpha_1, \beta_1)$. The first two possibilities imply that $q_1 = (\varepsilon_C, \varepsilon_C)$, which is a contradiction as then either $(\alpha, \beta) = (\alpha_1, \varepsilon_C)$ or (ε_C, β_1), both of which are indecomposable in $\Pi(\varphi, \psi)$. Hence $\sigma_1 = (\alpha_1, \beta_1)$.

Returning to (7), note that if $\alpha' = \varepsilon_A$, then $\beta' \in B^+$ with $\psi(\beta') = \varepsilon_C$, implying $\psi(\beta_1') = \psi(\beta_1) = \varepsilon_C$ also. This is a contradiction, as transitions of the form $(\iota, (\alpha_1, \beta_1), q)$ with $\psi(\beta_1) = \varepsilon_C$ are excluded from δ'. Similarly, $\beta' = \varepsilon_B$ also leads to a contradiction. Hence $\alpha' \in A^+$ and $\beta' \in B^+$.

Writing $(\alpha, \beta) = (a_1 a_2 \dots a_{|\alpha|}, b_1 b_2 \dots b_{|\beta|})$, then

$$(\alpha, \beta) = (a_1 \dots a_m, b_1 \dots b_n)(a_{m+1} \dots a_{|\alpha|}, b_{n+1} \dots b_{|\beta|}) \tag{8}$$

for some $1 \le m < |\alpha|$, $1 \le n < |\beta|$. In particular, as $a_1 \dots a_m \le_p \alpha$, $b_1 \dots b_n \le_p \beta$, then there exist minimal $M, N < |\alpha| + |\beta|$ such that $a_1 \dots a_m = \pi_{A^*}(\sigma_1 \dots \sigma_M)$ and $b_1 \dots b_n = \pi_{B^*}(\sigma_1 \dots \sigma_N)$. Taking $k = \min\{M, N\}$, it follows that

$$\sigma_1 \dots \sigma_k = \begin{cases} (a_1 \dots a_m, b_1 \dots b_{n'}) \text{ for some } n' < n & \text{if } k = M \\ (a_1 \dots a_{m'}, b_1 \dots b_n) \text{ for some } m' < m & \text{if } k = N. \end{cases}$$

If $k = M$, then as $\psi(b_1 \dots b_l) \le_p \psi(b_1 \dots b_n)$ for all $n' \le l \le n$ and $\psi(b_1 \dots b_n) = \varphi(a_1 \dots a_m)$, by Lemma 5.9 it follows that $q_{M+t} \in Q_1$ and hence

$\sigma_{M+t+1} = b_{n'+t+1}$ for $0 \le t < n - n'$. Thus $\sigma_1 \dots \sigma_{M+n-n'} = (a_1 \dots a_m, b_1 \dots b_n)$, and thus $q_{M+n-n'} = (\varepsilon_C, \varepsilon_C)$ by Lemma 5.9. But $M + n - n' = m + n < |\alpha| + |\beta|$, which contradicts acceptance of (α, β) by p (as there are no out-edges from $(\varepsilon_C, \varepsilon_C)$).

A similar proof shows if $k = N$, then $\sigma_1 \dots \sigma_{N+m-m'} = (a_1 \dots a_m, b_1 \dots b_n)$, and $q_{N+m-m'} = (\varepsilon_C, \varepsilon_C)$. But $N + m - m' = m + n < |\alpha| + |\beta|$, which again contradicts acceptance of (α, β) by p. Thus is must be that (α, β) is indecomposable, and hence $\mathcal{L}(\mathcal{A}_{\varphi,\psi})$ consists of indecomposables.

To show the reverse inclusion, let $(\alpha, \beta) \in \Pi(\varphi, \psi)$ be indecomposable. If $\alpha = \varepsilon_C$, then necessarily $\beta \in B$ and $\psi(\beta) = \varepsilon_C$, and the transition $(\iota, (\varepsilon_A, \beta), (\varepsilon_C, \varepsilon_C))$ accepts (α, β). Similarly, if $\beta = \varepsilon_C$, then $\alpha \in A$ with $\varphi(\alpha) = \varepsilon_C$, and the transition $(\iota, (\alpha, \varepsilon_B), (\varepsilon_C, \varepsilon_C))$ accepts (α, β). Otherwise, for $(\alpha, \beta) \in A^+ \times B^+$, define the sequence of triples $(q_{i-1}, \sigma_i, q_i)_{i=1}^{|\alpha|+|\beta|-1} \in Q \times \Sigma \times Q$ by $q_0 = \iota$, $\sigma_1 = (a_1, b_1)$, and

$$\sigma_i = \begin{cases} (a_{j_{i-1}}, \varepsilon_B) & \text{if } q_{i-1} \in Q_2 \\ (\varepsilon_A, b_{k_{i-1}}) & \text{if } q_{i-1} \in Q_1 \end{cases} \tag{9}$$

(where $j_{i-1} = |\pi_{A^*}(\sigma_1 \dots \sigma_{i-1})| + 1$, $k_{i-1} = |\pi_{B^*}(\sigma_1 \dots \sigma_{i-1})| + 1$ for $2 \le i \le |\alpha| + |\beta| - 1$), and

$$q_i = \begin{cases} (\Psi(\sigma_1 \dots \sigma_i)^{-1} \Phi(\sigma_1 \dots \sigma_i), \varepsilon_C) & \text{if } \Psi(\sigma_1 \dots \sigma_i) \le_p \Phi(\sigma_1 \dots \sigma_i) \\ (\varepsilon_C, \Phi(\sigma_1 \dots \sigma_i)^{-1} \Psi(\sigma_1 \dots \sigma_i)) & \text{if } \Phi(\sigma_1 \dots \sigma_i) \le_p \Psi(\sigma_1 \dots \sigma_i) \end{cases}$$

for $1 \leq i \leq |\alpha| + |\beta| - 1$.

Note that both q_i and σ_i are always well defined, as if $\varphi(\alpha) = \psi(\beta)$, then either $\Phi(\sigma_1 \dots \sigma_i) \leq_p \Psi(\sigma_1 \dots \sigma_i)$ or $\Psi(\sigma_1 \dots \sigma_i) \leq_p \Phi(\sigma_1 \dots \sigma_i)$, as $\Phi(\sigma_1 \dots \sigma_i)$ and $\Psi(\sigma_1 \dots \sigma_i)$ are prefixes of $\varphi(\alpha)$ and $\psi(\beta)$ respectively. Moreover, $\Phi(\sigma_1 \dots \sigma_i) \neq \Psi(\sigma_1 \dots \sigma_i)$ for $1 \leq i \leq |\alpha| + |\beta| - 1$ by indecomposability of (α, β), and hence $q_i \neq (\varepsilon_C, \varepsilon_C)$ for $0 \leq i \leq |\alpha| + |\beta| - 1$. By construction of σ_i, noting that if $\sigma_i \in A \times \{\varepsilon_B\}$, then

$$j_i = |\pi_{A^*}(\sigma_1 \dots \sigma_i)| + 1 = (|\pi_{A^*}(\sigma_1 \dots \sigma_{i-1})| + 1) + 1 = j_{i-1} + 1,$$

and

$$k_i = |\pi_{B^*}(\sigma_1 \dots \sigma_i)| + 1 = |\pi_{B^*}(\sigma_1 \dots \sigma_{i-1})| + 1 = k_{i-1},$$

whereas if $\sigma_i \in \{\varepsilon_A\} \times B$, then

$$j_i = |\pi_{A^*}(\sigma_1 \dots \sigma_i)| + 1 = (|\pi_{A^*}(\sigma_1 \dots \sigma_{i-1})| + 1 = j_{i-1},$$

and

$$k_i = |\pi_{B^*}(\sigma_1 \dots \sigma_i)| + 1 = (|\pi_{B^*}(\sigma_1 \dots \sigma_{i-1})| + 1) + 1 = k_{i-1} + 1.$$

As $j_1 = k_1 = 2$, then it follows that $\pi_{A^*}(\sigma_1 \dots \sigma_{|\alpha|+|\beta|-1}) = a_1 a_2 \dots a_m$ and $\pi_{B^*}(\sigma_1 \dots \sigma_{|\alpha|+|\beta|-1}) = b_1 b_2 \dots b_n$ for some $m \leq |\alpha|$, $n \leq |\beta|$. We conclude by making the following claims;

Claim 1: $(q_{i-1}, \sigma_i, q_i) \in \delta$ for $1 \leq i \leq |\alpha| + |\beta| - 1$,*hence* $(q_{i-1}, \sigma_i, q_i)_{i=1}^{|\alpha|+|\beta|-1}$*is a path in* $\mathcal{A}_{\varphi,\psi}$.

Claim 2: $\sigma_1 \dots \sigma_{|\alpha|+|\beta|-1} = (\alpha, \beta)$.

Combining the above claims, and noting that $q_0 = \iota$, $q_{|\alpha|+|\beta|-1} = (\varepsilon_C, \varepsilon_C)$ as $\varphi(\alpha) = \psi(\beta)$ and hence

$$\begin{aligned} &\Psi(\sigma_1 \dots \sigma_{|\alpha|+|\beta|-1})^{-1} \Phi(\sigma_1 \dots \sigma_{|\alpha|+|\beta|-1}) \\ &\quad = \Phi(\sigma_1 \dots \sigma_{|\alpha|+|\beta|-1})^{-1} \Psi(\sigma_1 \dots \sigma_{|\alpha|+|\beta|-1}) = \varepsilon_C, \end{aligned}$$

then there exists a path in $\mathcal{A}_{\varphi,\psi}$ accepting (α, β), and hence $(\alpha, \beta) \in \mathcal{L}(\mathcal{A}_{\varphi,\psi})$, completing the proof of the theorem.

Proof of Claim 1. For $i = 1$, $(q_0, \sigma_1, q_1) \in \delta$ by the definition, as necessarily $\sigma_1 = (a_1, b_1)$ and either $q_1 = (\Psi(\sigma_1)^{-1} \Phi(\sigma_1), \varepsilon_C) = (\psi(b_1)^{-1} \varphi(a_1), \varepsilon_C)$, or $q_1 = (\varepsilon_C, \Phi(\sigma_1)^{-1} \Psi(\sigma_1)) = (\varepsilon_C, \varphi(a_1)^{-1} \psi(b_1))$.

If $q_{i-1} \in Q_1$, then $q_{i-1} = (\Psi(\sigma_1 \dots \sigma_{i-1})^{-1} \Phi(\sigma_1 \dots \sigma_{i-1}), \varepsilon_C)$ and $\sigma_i = (\varepsilon_A, b_{k_i})$. As $\Psi(\sigma_1 \dots \sigma_i)$ and $\Phi(\sigma_1 \dots \sigma_i)$ are prefixes of $\psi(\beta) = \varphi(\alpha)$, then either $\Psi(\sigma_1 \dots \sigma_i) \leq_p \Phi(\sigma_1 \dots \sigma_i)$ or $\Phi(\sigma_1 \dots \sigma_i) \leq_p \Psi(\sigma_1 \dots \sigma_i)$.

If $\Psi(\sigma_1 \dots \sigma_i) \leq_p \Phi(\sigma_1 \dots \sigma_i)$, then in particular it follows that $\psi(b_{k_i}) = \Psi(\sigma_i) \leq_p \Psi(\sigma_1 \dots \sigma_{i-1})^{-1} \Phi(\sigma_1 \dots \sigma_{i-1})$, and

$$\begin{aligned} q_i &= (\Psi(\sigma_1 \dots \sigma_i)^{-1}\Phi(\sigma_1 \dots \sigma_i), \varepsilon_C) \\ &= ([\Psi(\sigma_1 \dots \sigma_{i-1})\Psi(\sigma_i)]^{-1}\Phi(\sigma_1 \dots \sigma_{i-1}), \varepsilon_C) \\ &= (\Psi(\sigma_i)^{-1}\Psi(\sigma_1 \dots \sigma_{i-1})^{-1}\Phi(\sigma_1 \dots \sigma_{i-1}), \varepsilon_C) \\ &= (\psi(b_{k_i})^{-1}\Psi(\sigma_1 \dots \sigma_{i-1})^{-1}\Phi(\sigma_1 \dots \sigma_{i-1}), \varepsilon_C), \end{aligned}$$

thus $(q_{i-1}, \sigma_i, q_i) \in \Delta_5 \subseteq \delta$ by definition. On the other hand, if $\Phi(\sigma_1 \dots \sigma_i) \leq_p \Psi(\sigma_1 \dots \sigma_i)$, then in particular it follows that $\Psi(\sigma_1 \dots \sigma_{i-1})^{-1}\Phi(\sigma_1 \dots \sigma_{i-1}) \leq_p \psi(b_{k_i})$, and

$$\begin{aligned} q_i &= (\varepsilon_C, \Phi(\sigma_1 \dots \sigma_i)^{-1}\Psi(\sigma_1 \dots \sigma_i)) \\ &= (\varepsilon_C, \Phi(\sigma_1 \dots \sigma_{i-1})^{-1}\Psi(\sigma_1 \dots \sigma_{i-1})\Psi(\sigma_i)) \\ &= (\varepsilon_C, [\Psi(\sigma_1 \dots \sigma_{i-1})^{-1}\Phi(\sigma_1 \dots \sigma_{i-1})]^{-1}\Psi(\sigma_i)) \\ &= (\varepsilon_C, [\Psi(\sigma_1 \dots \sigma_{i-1})^{-1}\Phi(\sigma_1 \dots \sigma_{i-1})]^{-1}\psi(b_{k_i})), \end{aligned}$$

thus $(q_{i-1}, \sigma_i, q_i) \in \Delta_6 \subseteq \delta$ by definition.

If $q_{i-1} \in Q_2$, then a similar proof shows that $(q_{i-1}, \sigma_i, q_i) \in \Delta_6 \cup \Delta_8 \subseteq \delta$, thus proving the claim.

Proof of Claim 2. It suffices to prove that $m = |\alpha|$, and $n = |\beta|$. Let S_A, S_B be defined by

$$\begin{aligned} S_A &:= \{i \in \{2, \dots, |\alpha| + |\beta| - 1\} \,:\, \sigma_i \in A \times \{\varepsilon_B\}\} \\ S_B &:= \{i \in \{2, \dots, |\alpha| + |\beta| - 1\} \,:\, \sigma_i \in \{\varepsilon_A\} \times B\} \end{aligned}$$

Then $m = |S_A| + 1$ and $n = |S_B| + 1$. Suppose for a contradiction that $|S_A| > |\alpha| - 1$. Ordering S_A in the natural way, let $I \in S_A$ be the element at position $|\alpha|$. Then

$$|\pi_{A^*}(\sigma_1 \dots \sigma_{I-1})| = |\pi_{A^*}(\sigma_2 \dots \sigma_{I-1})| + 1 = |\pi_{A^*}(\sigma_2 \dots \sigma_I)| - 1 + 1 = |\alpha|.$$

Moreover, as $\pi_{A^*}(\sigma_1 \dots \sigma_{I-1}) \leq_p a_1 a_2 \dots a_m$, it follows that $\pi_{A^*}(\sigma_1 \dots \sigma_{I-1}) = a_1 a_2 \dots a_{|\alpha|}$. In particular, $\Phi(\sigma_1 \dots \sigma_{I-1}) = \varphi(\alpha)$. But

$$\begin{aligned} &\varphi(\alpha) = \psi(\beta) \\ &\Rightarrow \Psi(\sigma_1 \dots \sigma_{I-1}) \leq_p \Phi(\sigma_1 \dots \sigma_{I-1}) \\ &\Rightarrow q_{I-1} \in Q_1. \end{aligned}$$

As $q_{I-1} \in Q_1$, then $\sigma_I \in \{\varepsilon_A\} \times B$, which is a contradiction, as then $I \notin S_A$. Hence $|S_A| \leq |\alpha| - 1$. A similar proof shows that $|S_B| \leq |\beta| - 1$. Moreover, as $|S_A| + |S_B| = |\alpha| - 1 + |\beta| - 1$, it follows that $|S_A| \nless |\alpha| - 1$ (for otherwise $|S_B| > |\beta| - 1$), and similarly $|S_B| \nless |\beta| - 1$. Hence $|S_A| = |\alpha| - 1$, $|S_B| = |\beta| - 1$ which gives $m = |\alpha|$, $n = |\beta|$ as required. □

Proof of Theorem 5.6 ($\Rightarrow$) For sufficiency, we prove the contrapositive. Suppose that $\mathcal{A}_{\varphi,\psi}$ has a cycle. Then there exists a sequence of transitions $(q_{i-1}, \sigma_i, q_i)_{i=1}^k$ where $q_0 = q_k$. By the definition of δ, it follows that $q_0 \neq \imath$ and $q_0 \neq (\varepsilon_C, \varepsilon_C)$. Thus either

$q_0 = (u, \varepsilon_C)$ where $u \in C^+$ is such that $u <_s w$ for some $w \in \varphi(A)$, or $q_0 = (\varepsilon_C, v)$ where $v \in C^+$ is such that $v <_s w$ for some $w \in \psi(B)$.

It suffices to consider the case where $q_0 = (u, \varepsilon_C)$, as the proof for the other case will follow by a symmetric argument. As u is a suffix of $w = \varphi(a)$ for some $a \in A$, and ψ is surjective, then there exist $b_1, \dots, b_j, b'_1, \dots, b'_l \in B$ such that $\psi(b_1 \dots b_j)u = w$ and $\psi(b'_1 \dots b'_l) = u$.

Construct the sequences of transitions $(p_{i-1}, \tau_i, p_i)_{i=1}^{j}$ and $(r_{i-1}, \rho_i, r_i)_{i=1}^{l}$ where

(1) $(p_0, \tau_1, p_1) = (\iota, (a, b_1), ([\psi(b_1)]^{-1}w, \varepsilon_C))$,
(2) $p_i = ([\psi(b_1 ... b_i)]^{-1}w, \varepsilon_C)$, $\tau_i = (\varepsilon_A, b_i)$ for $1 < i \leq j$,
(3) $r_0 = q_0$, $\rho_i = (\varepsilon_A, b'_i)$, $r_i = ([\psi(b'_1 \dots b'_i)]^{-1}u, \varepsilon_C)$ for $1 \leq i \leq l$.

Noting that $p_j = q_0 = q_k = r_0$ and $r_l = (\varepsilon_C, \varepsilon_C)$, then for all $n \in \mathbb{N}$ it follows that the input $\tau_1 \dots \tau_{j+1}(\sigma_1 \dots \sigma_k)^n \rho_1 \dots \rho_l$ is accepted by $\mathcal{A}_{\varphi,\psi}$, via the concatenation of the sequences of transitions $(p_{i-1}, \tau_i, p_i)_{i=1}^{j}$, $(q_{i-1}, \sigma_i, q_i)_{i=1}^{k}$ (n times), and $(r_{i-1}, \rho_i, r_i)_{i=1}^{l}$.

($\Leftarrow$) For necessity, suppose that $\mathcal{A}_{\varphi,\psi}$ has no cycles. Then as $|Q|, |\delta| < \infty$, it follows that there are only finitely many transitions in $\mathcal{A}_{\varphi,\psi}$, and hence $|\mathcal{L}(\mathcal{A}_{\varphi,\psi})| < \infty$. By Corollary 5.11, it follows that $\Pi(\varphi, \psi)$ has finitely many indecomposable elements. Hence by Lemma 4.2, $\Pi(\varphi, \psi)$ is finitely generated as required. $\square$

We also give an analogous result for fiber products of two finitely generated free semigroups over a finitely generated free semigroup fiber. Given epimorphisms $\varphi : A^+ \to C^+$, $\psi : B^+ \to C^+$ (with A, B, C finite alphabets), we can extend φ and ψ naturally to homomorphisms $\varphi' : A^* \to C^*$, $\psi' : B^* \to C^*$ by mapping ε_A and ε_B to ε_C. Then $\Pi(\varphi', \psi') = \Pi(\varphi, \psi) \cup \{(\varepsilon_A, \varepsilon_B)\}$, and hence $\Pi(\varphi, \psi)$ is finitely generated as a semigroup if and only if $\Pi(\varphi', \psi')$ is finitely generated as a monoid. Hence we obtain the following corollaries:

Corollary 5.11 *Let $\varphi : A^+ \to C^+$, $\psi : B^+ \to C^+$ be two epimorphisms with A, B, C finite alphabets. Then the language accepted by $\mathcal{A}_{\varphi',\psi'}$ is the set of indecomposable elements of $\Pi(\varphi, \psi)$.*

Corollary 5.12 *Let $\varphi : A^+ \to C^+$, $\psi : B^+ \to C^+$ be two epimorphisms with A, B, C finite alphabets. Then the fiber product of A^+ with B^+ over C^+ with respect to φ, ψ is finitely generated if and only if $\mathcal{A}_{\varphi',\psi'}$ has no cycles.*

6 Some remarks on numbers of subdirect products

Though the results above appear to indicate that finitely generated fiber products of free semigroups are sparse, we know that finitely generated subdirect products of finitely generated free semigroups are easy to come by. For example, let A, B be finite alphabets. Then choosing $X \subseteq A \times B$ such that the natural projection maps $\pi_A : X \to A$ and $\pi_B : X \to B$ are surjections yields subdirect products $\langle X \rangle$ of A^+ and B^+. It is then possible to count all such X, as in the next result.

Proposition 6.1 *Let A, B be finite sets, and let*

$$\mathrm{Subdirect}(A, B) := \{X \subseteq A \times B : \langle X \rangle \leq_{\mathrm{sd}} A^+ \times B^+\}.$$

Then

$$|\mathrm{Subdirect}(A, B)| = \sum_{i=0}^{|A|} (-1)^i \binom{|A|}{i} (2^{|A|-i} - 1)^{|B|}. \tag{10}$$

Moreover,

$$\lim_{|A| \to \infty} \frac{|\mathrm{Subdirect}(A, A)|}{|\mathcal{P}(A \times A)|} = 1.$$

Proof Without loss of generality, as A and B are finite we can relabel A and B so that $A = \{a_1, \dots, a_m\}$ and $B = \{b_1, \dots, b_n\}$ for some $m, n \in \mathbb{N}$. We can associate any $X \in \mathrm{Subdirect}(A, B)$ to the binary m by n matrix M_X defined by

$$(M_X)_{i,j} = \begin{cases} 1 & \text{if } (a_i, b_j) \in X \\ 0 & \text{otherwise} \end{cases}.$$

In particular, as $\langle X \rangle$ is a subdirect product of A^+ and B^+, then every $a_i \in A$ is paired with at least one $b_j \in B$, and vice versa. Hence M_X has no zero rows or columns. Conversely, we can identify every binary m by n matrix M with no zero rows or columns to a subset $X_M \in \mathrm{Subdirect}(A, B)$, where

$$X_M := \{(a_i, b_j) \in A \times B : (M)_{i,j} = 1\}.$$

Hence $|\mathrm{Subdirect}(A, B)|$ is equal to the number of binary m by n matrices with no zero rows or columns. Thus (10) follows by a standard inclusion exclusion argument.

Moreover, for the limit, as $\mathrm{Subdirect}(A, A) \subseteq \mathcal{P}(A \times A)$, then

$$\frac{|\mathrm{Subdirect}(A, A)|}{|\mathcal{P}(A \times A)|} \leq 1. \tag{11}$$

On the other hand, as

$$|\mathrm{Subdirect}(A, A)| = (2^{|A|} - 1)^{|A|} - |A|(2^{|A|-1} - 1)^{|A|} + \sum_{i=2}^{|A|} (-1)^i \binom{|A|}{i} (2^{|A|-i} - 1)^{|A|}, \tag{12}$$

then by verifying that the summand values $x_i := \binom{|A|}{i}(2^{|A|-i} - 1)^{|A|}$ form a strictly decreasing sequence $(x_i)_{i=2}^{|A|}$, we see that

$$\sum_{i=2}^{|A|}(-1)^i\binom{|A|}{i}(2^{|A|-i}-1)^{|A|} \geq 0,$$

implying from (12) that

$$|\mathrm{Subdirect}(A,A)| \geq (2^{|A|}-1)^{|A|} - |A|(2^{|A|-1}-1)^{|A|}.$$

Thus as

$$\begin{aligned}\left(1-\frac{1}{2^{|A|}}\right)^{|A|} - \frac{|A|}{2^{|A|}} &= \frac{(2^{|A|}-1)^{|A|} - |A|(2^{|A|-1})^{|A|}}{2^{|A|^2}}\\ &\leq \frac{(2^{|A|}-1)^{|A|} - |A|(2^{|A|-1}-1)^{|A|}}{2^{|A|^2}},\end{aligned}$$

then

$$\left(1-\frac{1}{2^{|A|}}\right)^{|A|} - \frac{|A|}{2^{|A|}} \leq \frac{|\mathrm{Subdirect}(A,A)|}{|\mathcal{P}(A\times A)|} \leq 1,$$

from which the limit follows from standard analytic arguments. □

Proposition 6.1 suggests that finitely generated subdirect products are numerous within the class of subsemigroups of $A^+ \times B^+$ generated by subsets of $A \times B$, as $|A|$ grows with $|B|$. It is natural to ask how many of those finitely generated subdirect products are fiber products (using Lemma 2.1), and what proportion of all such subdirect products they constitute. This is answered in the following result.

Proposition 6.2 *Let A, B be finite sets, and let*

$$\begin{aligned}\mathrm{Subdirect}(A,B) &:= \{X \subseteq A\times B : \langle X\rangle \leq_{\mathrm{sd}} A^+ \times B^+\},\\ \mathrm{Fiber}(A,B) &:= \{X \subseteq \mathrm{Subdirect}(A,B) : \ker\pi_{A^+}\circ\ker\pi_{B^+} = \ker\pi_{B^+}\circ\ker\pi_{A^+}\}.\end{aligned}$$

Then

$$|\mathrm{Fiber}(A,B)| = \sum_{i=1}^{\min\{|A|,|B|\}} i!\, S(|A|,i)S(|B|,i), \tag{13}$$

where $S(n,k)$ is the Stirling number of the second kind.

Moreover,

$$\lim_{|A|\to\infty}\frac{|\mathrm{Fiber}(A,A)|}{|\mathrm{Subdirect}(A,A)|} = 0.$$

Proof We claim that $|\mathrm{Fiber}(A,B)|$ is equal to the number of binary $m\times n$ matrices with no zero rows, zero columns, or submatrices of the form

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}. \tag{14}$$

To prove this, without loss of generality, let $A = \{a_1, \dots, a_m\}$, and $B = \{b_1, \dots, b_n\}$. We can associate an $m \times n$ binary matrix M_X to each $X \in \text{Fiber}(A, B)$ as in Proposition 6.1. In particular, M_X has no zero rows or columns.

Any two non-zero entries in the same row of M_X correspond to two generating pairs $(a_i, b_j), (a_{i'}, b_{j'}) \in \langle X \rangle$ with $i = i'$, and hence correspond to generating pairs which are related by the congruence $\ker \pi_{A^+}$. Similarly, any two non-zero entries in the same column of M_X correspond to two generating pairs which are related by the congruence $\ker \pi_{B^+}$. Hence there are no submatrices of M_X of the type given in (14) as these correspond to pairs $(a_i, b_j), (a_{i'}, b_{j'}) \in X$ which are related by $\ker \pi_{A^+} \circ \ker \pi_{B^+}$ but not by $\ker \pi_{B^+} \circ \ker \pi_{A^+}$, or vice versa.

Conversely, let $((u, v), (u', v')) \in \langle X \rangle \times \langle X \rangle$. As

$$((u, v), (u', v')) \in \ker \pi_{A^+} \circ \ker \pi_{B^+} \Leftrightarrow ((u_i, v_i), (u'_i, v'_i)) \in \ker \pi_{A^+} \circ \ker \pi_{B^+}$$

for $1 \leq i \leq |u|$, and similarly

$$((u, v), (u', v')) \in \ker \pi_{B^+} \circ \ker \pi_{A^+} \Leftrightarrow ((u_i, v_i), (u'_i, v'_i)) \in \ker \pi_{B^+} \circ \ker \pi_{A^+}$$

for $1 \leq i \leq |u|$, then the congruences $\ker \pi_{A^+}$ and $\ker \pi_{B^+}$ on $\langle X \rangle$ are completely determined by their restrictions to X, and hence so are $\ker \pi_{A^+} \circ \ker \pi_{B^+}$ and $\ker \pi_{B^+} \circ \ker \pi_{A^+}$. Hence every binary matrix without 2×2 submatrices of the type given in (14) corresponds to a fiber product of A^+ with B^+. This proves the claim.

The number of $m \times n$ binary matrices allowing for zero rows and columns without submatrices of the above form has been given in [8, Theorem 3.1] as

$$\sum_{i=0}^{\min\{m,n\}} i!\, S(m+1, i+1) S(n+1, i+1).$$

via transforming each matrix into a block diagonal binary matrix, and associating this matrix with two set partitions μ and ν of $\{1, \dots m+1\}$ and $\{1, \dots, n+1\}$ into $i+1$ blocks for some $i \in \mathbb{N}$, and a permutation on $\{1, \dots, i\}$. Noting that matrices with no zero rows or columns that avoid the set of submatrices given in (14) can be transformed into block diagonal matrices without any zero blocks on the diagonal, and accounting for this in the proof of [8, Theorem 3.1] gives the result in (13).

For the limit, as $S(n, k)$ is the number of ways to partition a set of size n into k non-empty blocks, which is less than the number of ways to assign a set of size n objects to k unlabelled bins (allowing for empty bins), then we get the following upper bound on the number of fiber products.

$$|\text{Fiber}(A, A)| = \sum_{i=1}^{|A|} i!\, S(|A|, i)^2 \leq \sum_{i=1}^{|A|} i! \left(\frac{i^{|A|}}{i!} \right)^2 \leq \sum_{i=1}^{|A|} i^{2|A|} \leq |A|.|A|^{2|A|} = |A|^{2|A|+1}.$$

Hence using Proposition 6.1, we have

$$\lim_{|A|\to\infty} \frac{|\mathrm{Fiber}(A,A)|}{|\mathrm{Subdirect}(A,A)|} = \lim_{|A|\to\infty} \frac{|\mathrm{Fiber}(A,A)|}{2^{|A|^2}} \leq \lim_{|A|\to\infty} \frac{|A|^{2|A|+1}}{2^{|A|^2}}$$

which tends to zero by standard analytic arguments. □

7 Further questions

Most of the results in this paper indicate that fiber products of free semigroups are rarely finitely generated, though finitely generated subdirect products of free semigroups are abundant. The quotient can be defined for these non-fiber products, but it does not determine the semigroup in the same way as the fiber product. Moreover, the results limit the possible presentations for fiber quotients of finitely generated fiber products of free semigroups. These observations motivate the following open questions:

Question 7.1 Does there exist a finitely generated subdirect product of two free monoids with a finite quotient, which is not finitely presented?

Question 7.2 Given a subdirect product S of two free semigroups by a finite set of generating pairs, is it decidable whether or not S is a fiber product?

Question 7.3 Does Theorem 3.5 generalise to infinite fiber quotients? That is, is a finitely generated fiber product of two free semigroups with an infinite fiber quotient also finitely presented?

Acknowledgements The author would like to particularly thank Professor Nik Ruškuc for his ever supportive guidance during the writing of this paper. For my aunt, Jacky.

References

1. Baumslag, G., Roseblade, J.E.: Subgroups of direct products of free groups. J. London Math. Soc. **30**, 44–52 (1984)
2. Bridson, M.R., Miller III, C.F.: Structure and finiteness properties of subdirect products of groups. Proc. Lond. Math. Soc. **98**, 631–651 (2009)

3. Burris, S., Sankappanavar, H.P.: A Course in Universal Algebra. Graduate Texts in Mathematics, vol. 78. Springer, New York (1981)
4. Clayton, A., Ruskuc, N.: On the number of subsemigroups of direct products involving the free monogenic semigroup. J. Austral. Math. Soc. **109**, 24–35 (2020)
5. Goursat, É.: Sur les substitutions orthogonales et les divisions régulières de l'espace. Annales Scientifiques de l'École Normale Supérieure **6**, 9–102 (1889)
6. Grunewald, F.J.: On some groups which cannot be finitely presented. J. London Math. Soc. **17**, 427–436 (1978)
7. Howie, J.M.: Fundamentals of Semigroup Theory. LMS Monographs, vol. 12. The Clarendon Press, New York (1995)
8. Hyeong-Kwan, J., Seunghyun, S.: Enumeration of $0/1$-matrices avoiding some 2×2 matrices, arXiv:1107.1299
9. Mayr, P., Ruškuc, N.: Generating subdirect products. J. London Math. Soc. **100**, 404–424 (2019)
10. Mikhaĭlova, K.A.: The occurrence problem for direct products of groups, *Mat. Sb. (N.S.)* **70(112)**, 241–251 (1966) (**In Russian**)